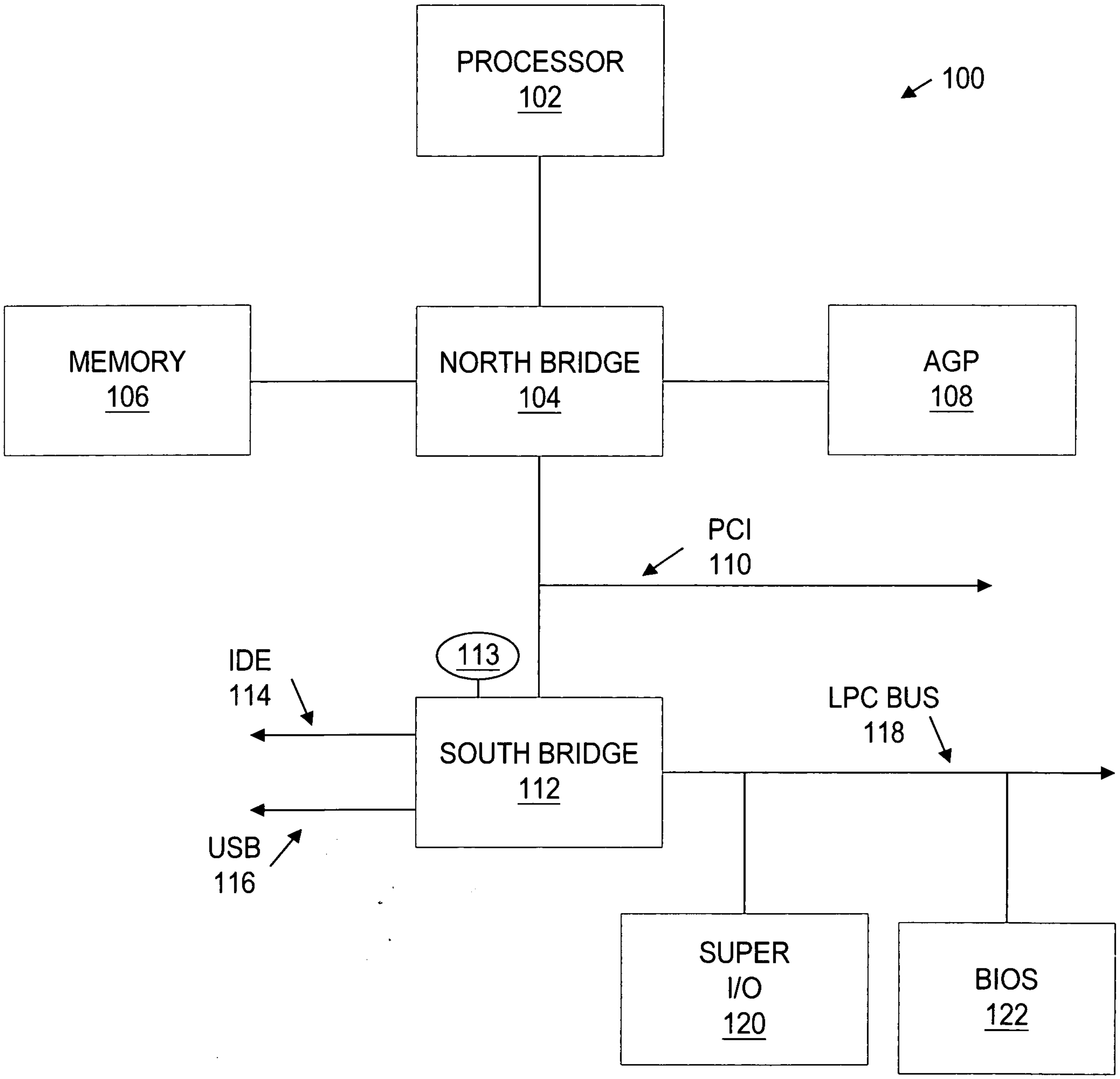


Fig. 1A
(Prior Art)

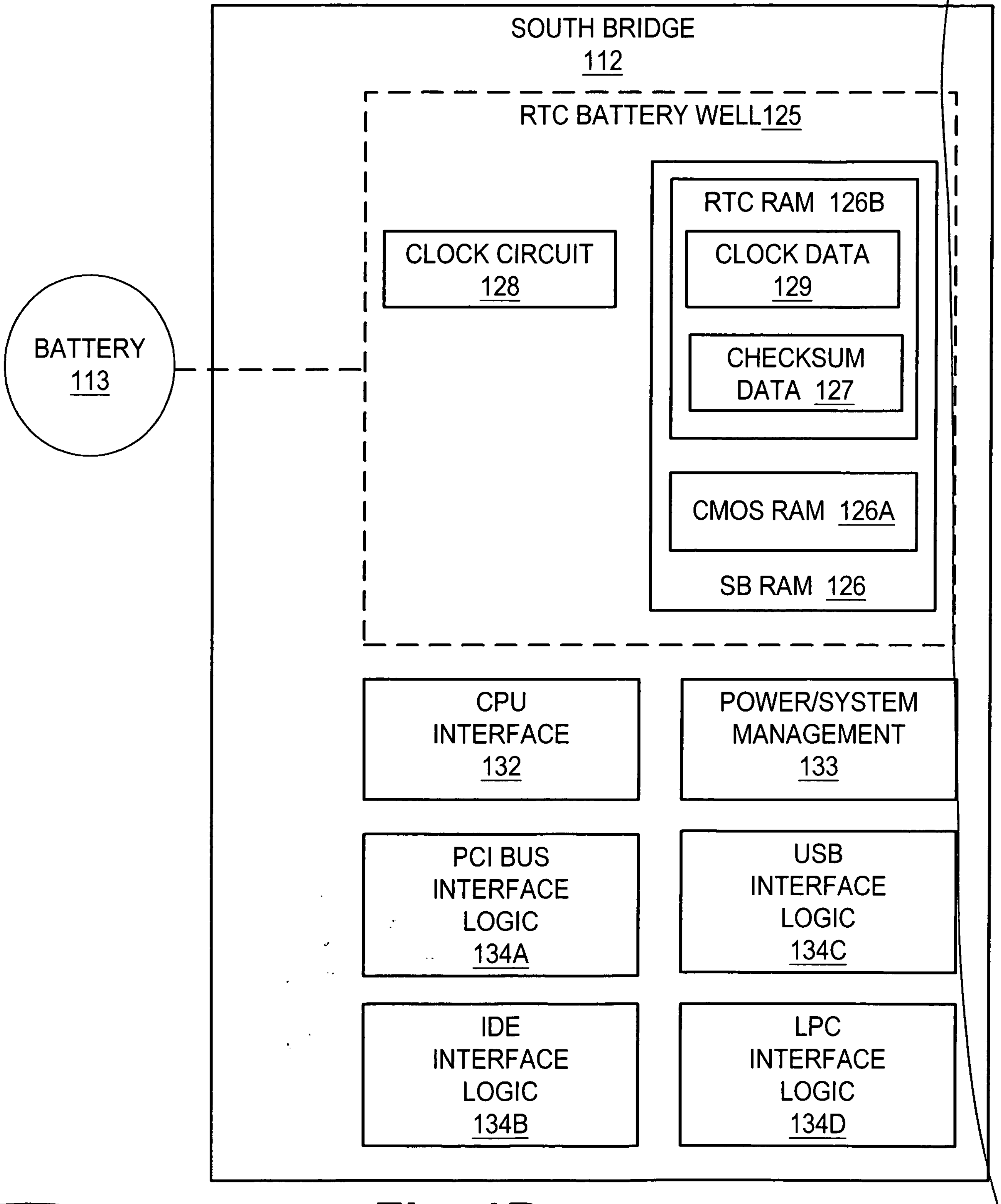


Fig. 1B
(Prior Art)

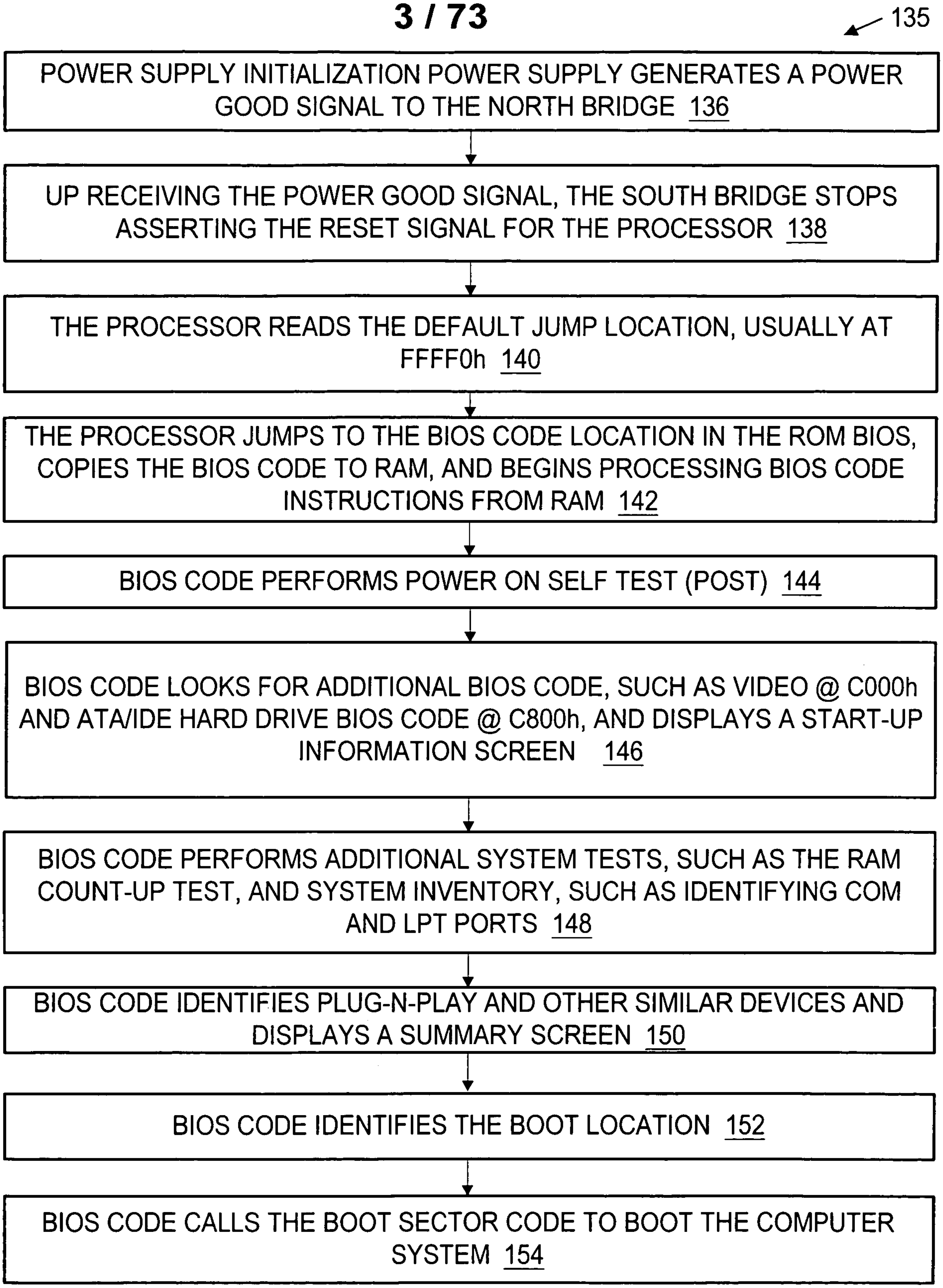

135
POWER SUPPLY INITIALIZATION POWER SUPPLY GENERATES A POWER GOOD SIGNAL TO THE NORTH BRIDGE 136
UP RECEIVING THE POWER GOOD SIGNAL, THE SOUTH BRIDGE STOPS ASSERTING THE RESET SIGNAL FOR THE PROCESSOR 138
THE PROCESSOR READS THE DEFAULT JUMP LOCATION, USUALLY AT FFFF0h 140
THE PROCESSOR JUMPS TO THE BIOS CODE LOCATION IN THE ROM BIOS, COPIES THE BIOS CODE TO RAM, AND BEGINS PROCESSING BIOS CODE INSTRUCTIONS FROM RAM 142
BIOS CODE PERFORMS POWER ON SELF TEST (POST) 144
BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 146
BIOS CODE PERFORMS ADDITIONAL SYSTEM TESTS, SUCH AS THE RAM COUNT-UP TEST, AND SYSTEM INVENTORY, SUCH AS IDENTIFYING COM AND LPT PORTS 148
BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 150
BIOS CODE IDENTIFIES THE BOOT LOCATION 152
BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 154

Fig. 2A
(Prior Art)

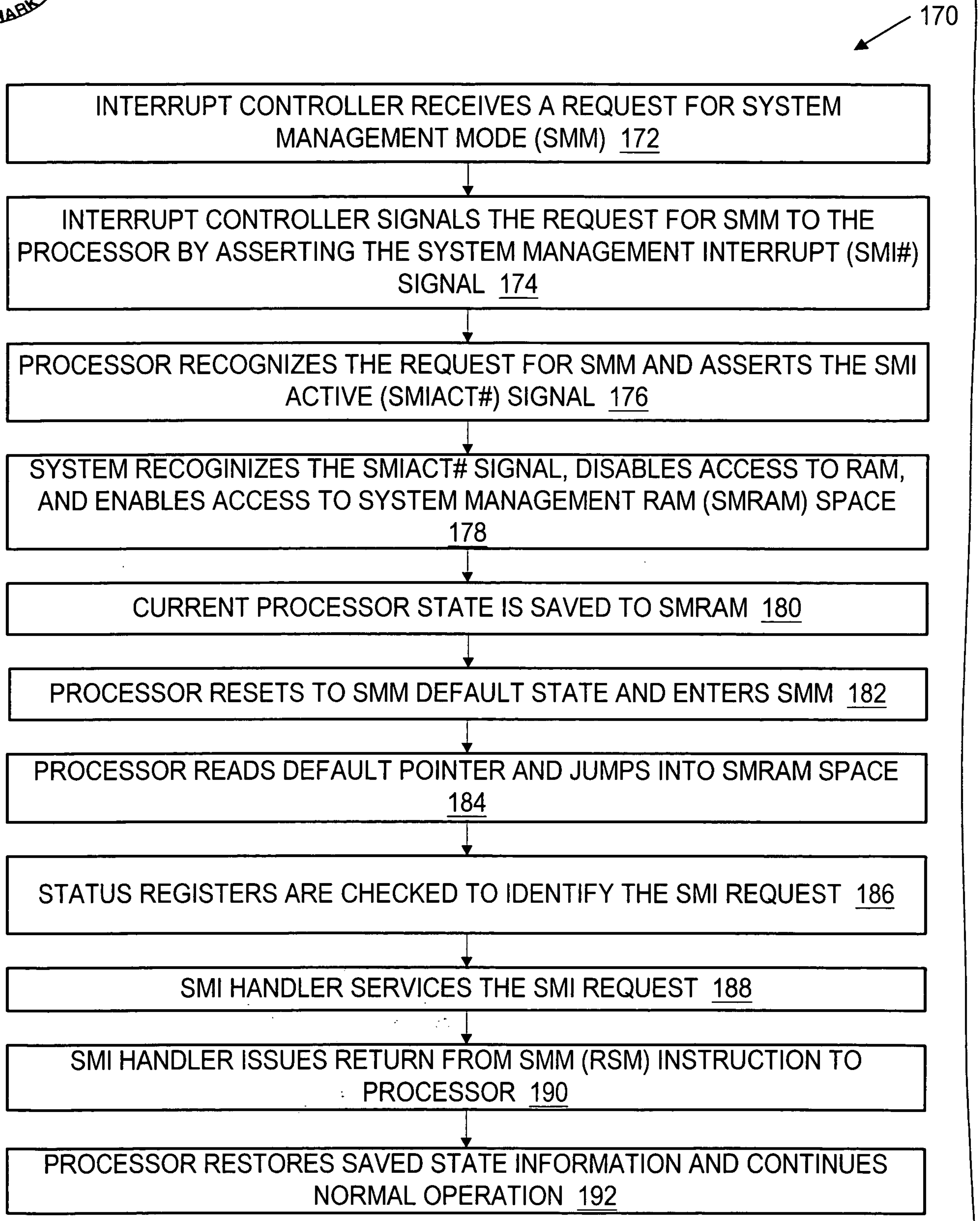

170
INTERRUPT CONTROLLER RECEIVES A REQUEST FOR SYSTEM MANAGEMENT MODE (SMM) 172
INTERRUPT CONTROLLER SIGNALS THE REQUEST FOR SMM TO THE PROCESSOR BY ASSERTING THE SYSTEM MANAGEMENT INTERRUPT (SMI#) SIGNAL 174
PROCESSOR RECOGNIZES THE REQUEST FOR SMM AND ASSERTS THE SMI ACTIVE (SMIACT#) SIGNAL 176
SYSTEM RECOGINIZES THE SMIACT# SIGNAL, DISABLES ACCESS TO RAM, AND ENABLES ACCESS TO SYSTEM MANAGEMENT RAM (SMRAM) SPACE 178
CURRENT PROCESSOR STATE IS SAVED TO SMRAM 180
PROCESSOR RESETS TO SMM DEFAULT STATE AND ENTERS SMM 182
PROCESSOR READS DEFAULT POINTER AND JUMPS INTO SMRAM SPACE 184
STATUS REGISTERS ARE CHECKED TO IDENTIFY THE SMI REQUEST 186
SMI HANDLER SERVICES THE SMI REQUEST 188
SMI HANDLER ISSUES RETURN FROM SMM (RSM) INSTRUCTION TO PROCESSOR 190
PROCESSOR RESTORES SAVED STATE INFORMATION AND CONTINUES NORMAL OPERATION 192

Fig. 2B
(Prior Art)

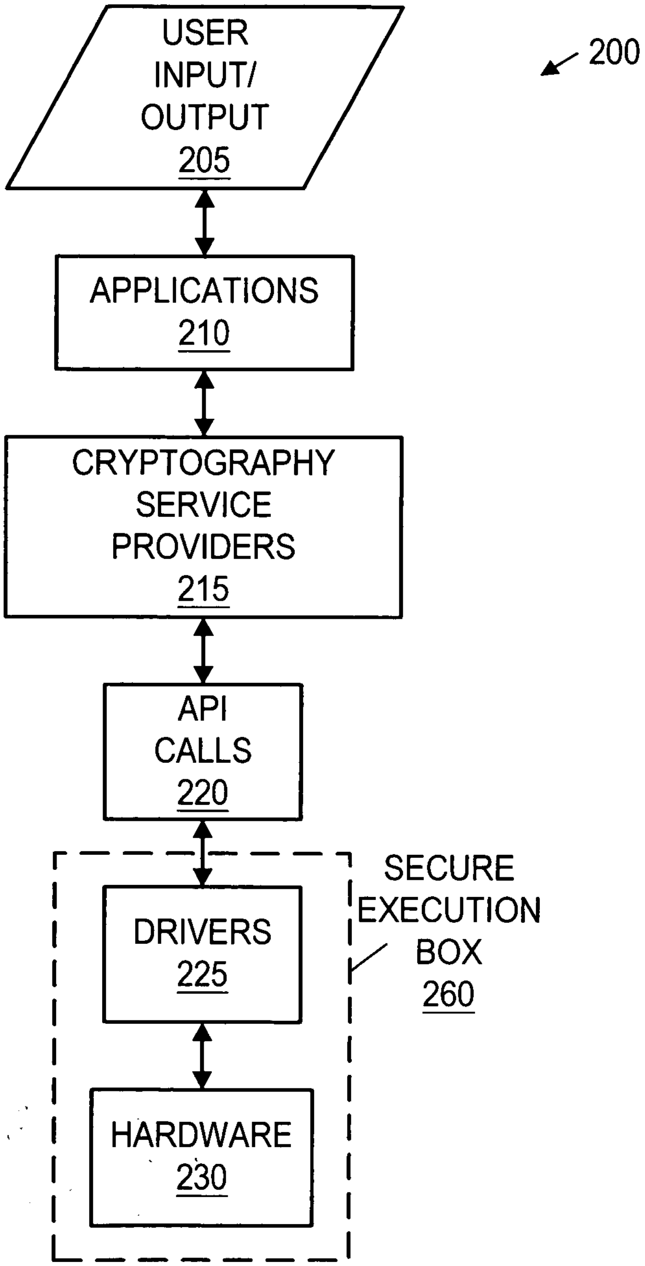

200
USER INPUT/ OUTPUT 205
APPLICATIONS 210
CRYPTOGRAPHY SERVICE PROVIDERS 215
API CALLS 220
DRIVERS 225
HARDWARE 230
SECURE EXECUTION BOX 260

Fig. 3 2

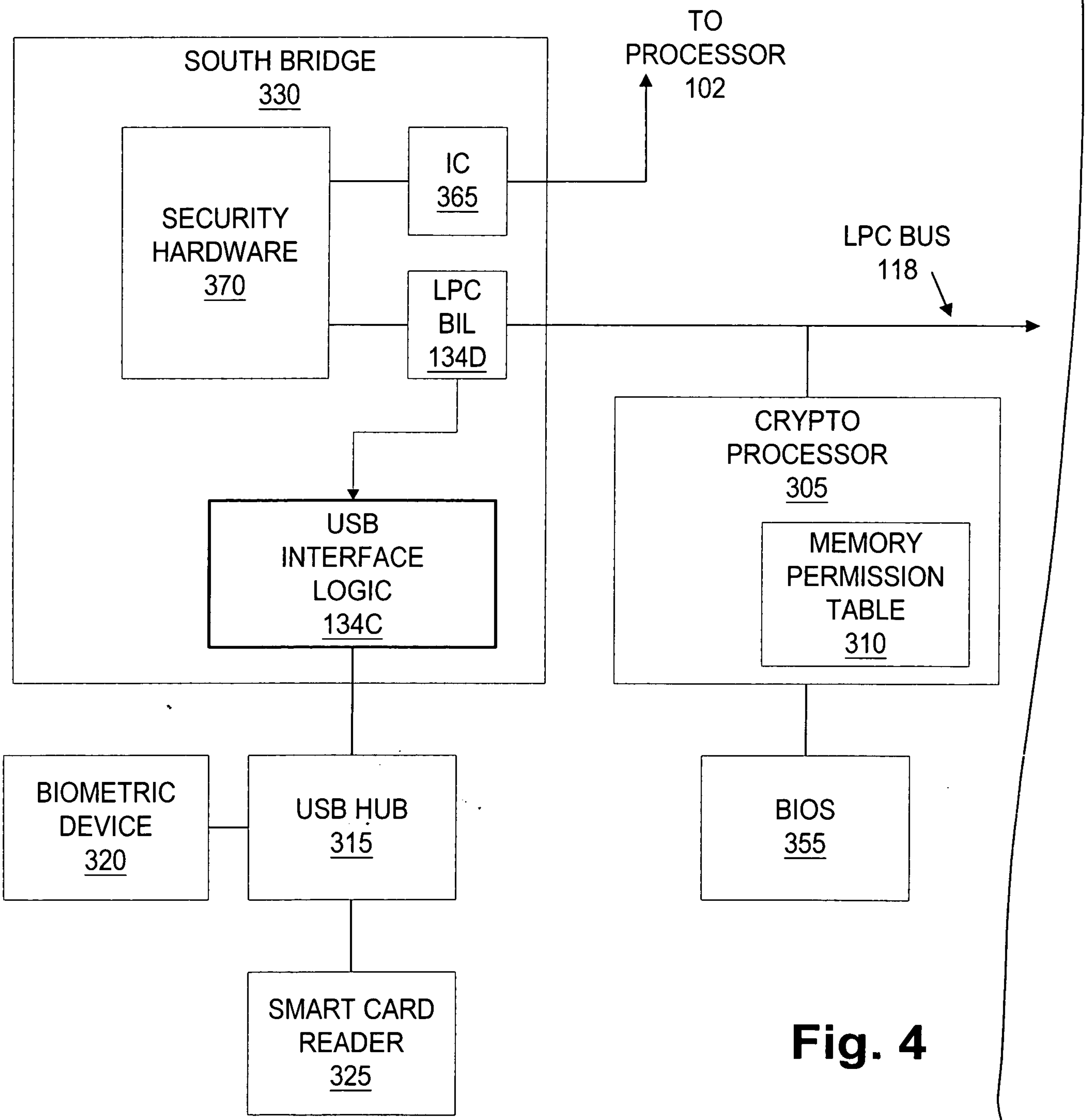

SOUTH BRIDGE
330
SECURITY
HARDWARE
370
IC
365
TO
PROCESSOR
102
LPC
BIL
134D
LPC BUS
118
USB
INTERFACE
LOGIC
134C
CRYPTO
PROCESSOR
305
MEMORY
PERMISSION
TABLE
310
BIOMETRIC
DEVICE
320
USB HUB
315
BIOS
355
SMART CARD
READER
325

Fig. 4

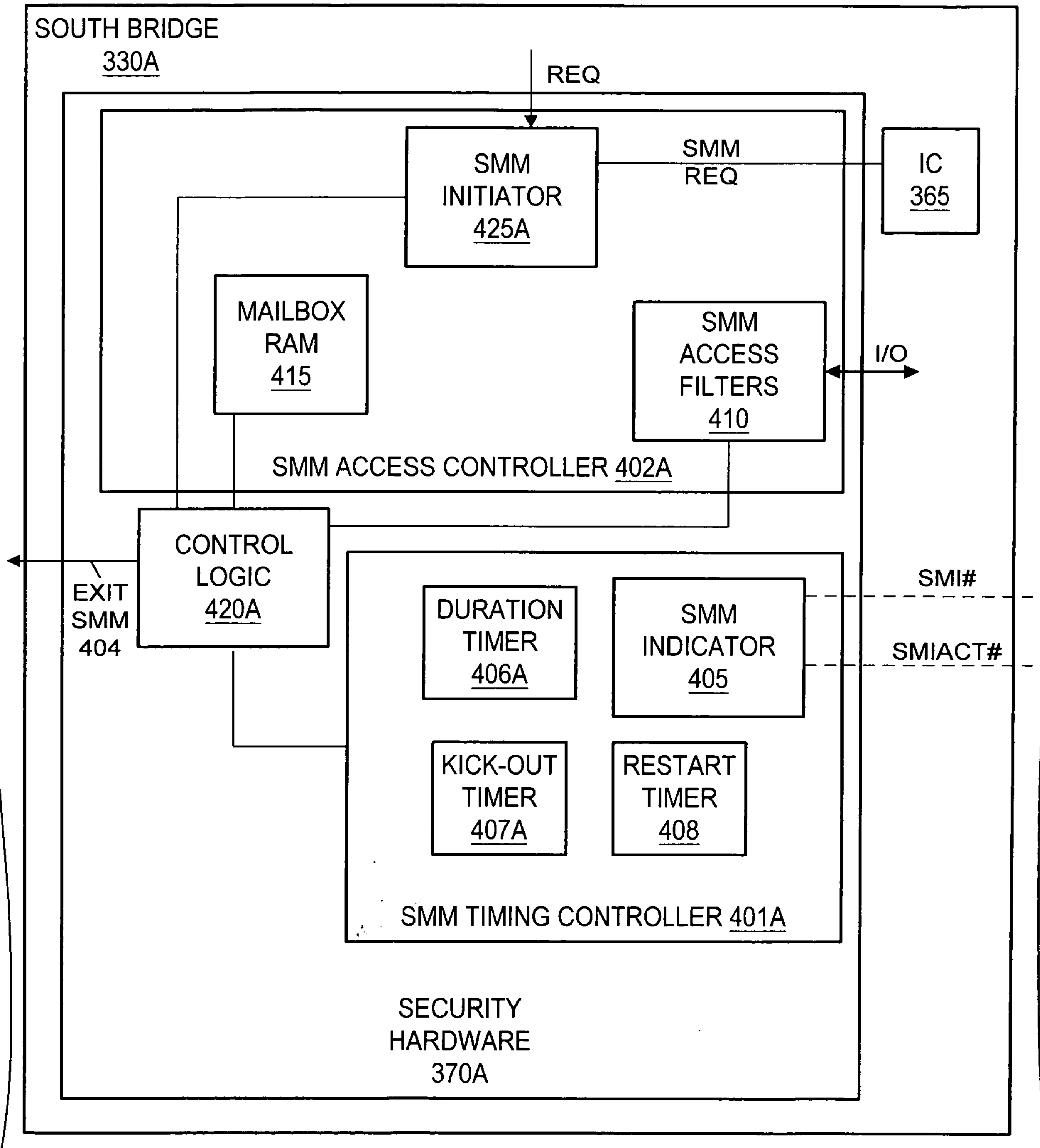

SOUTH BRIDGE
330A
REQ
SMM
INITIATOR
425A
SMM
REQ
IC
365
MAILBOX
RAM
415
SMM
ACCESS
FILTERS
410
I/O
SMM ACCESS CONTROLLER 402A
CONTROL
LOGIC
420A
EXIT
SMM
404
DURATION
TIMER
406A
SMM
INDICATOR
405
SMI#
SMIACT#
KICK-OUT
TIMER
407A
RESTART
TIMER
408
SMM TIMING CONTROLLER 401A
SECURITY
HARDWARE
370A

Fig. 5A

Strongin / TT3766

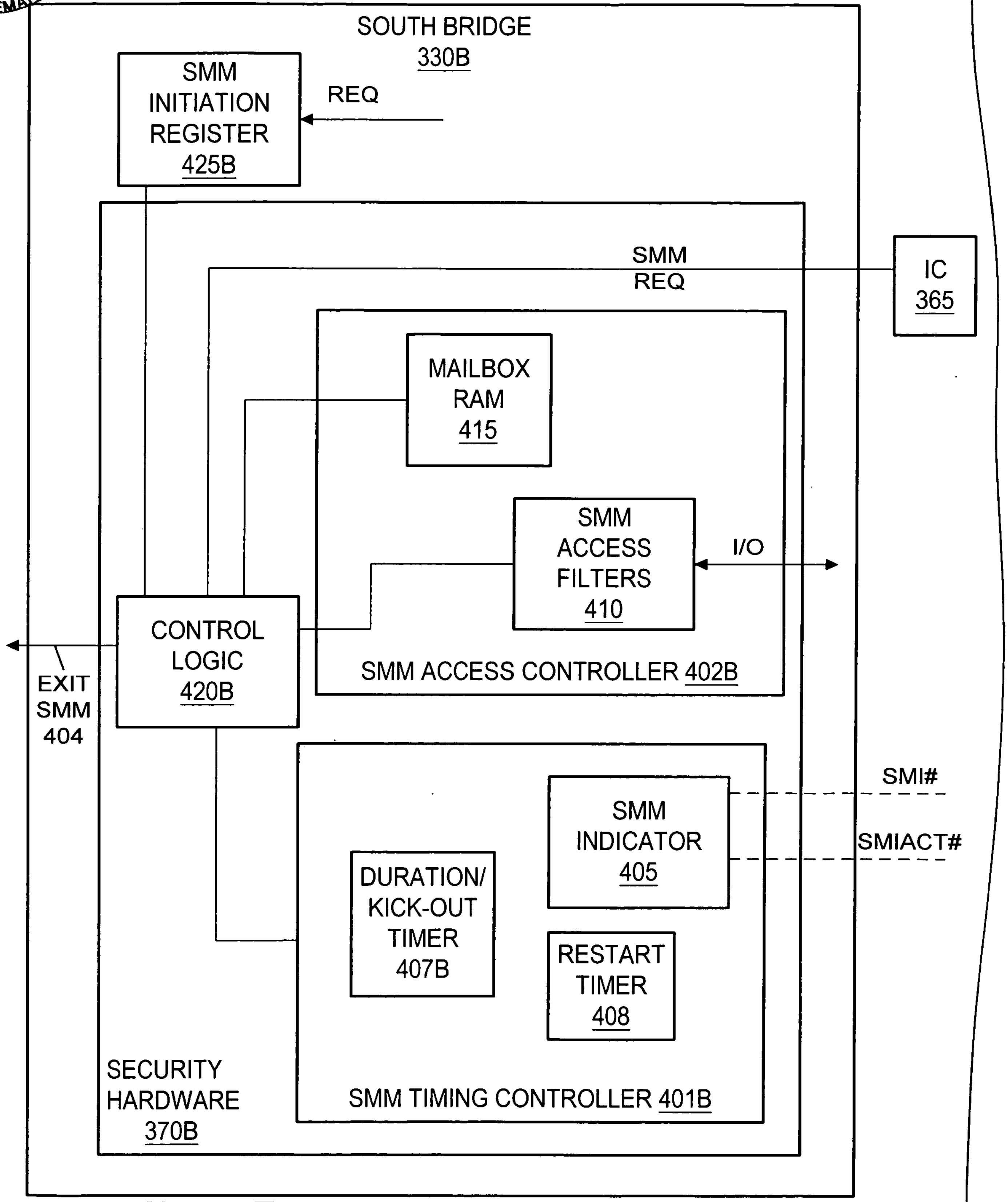


Fig. 5B

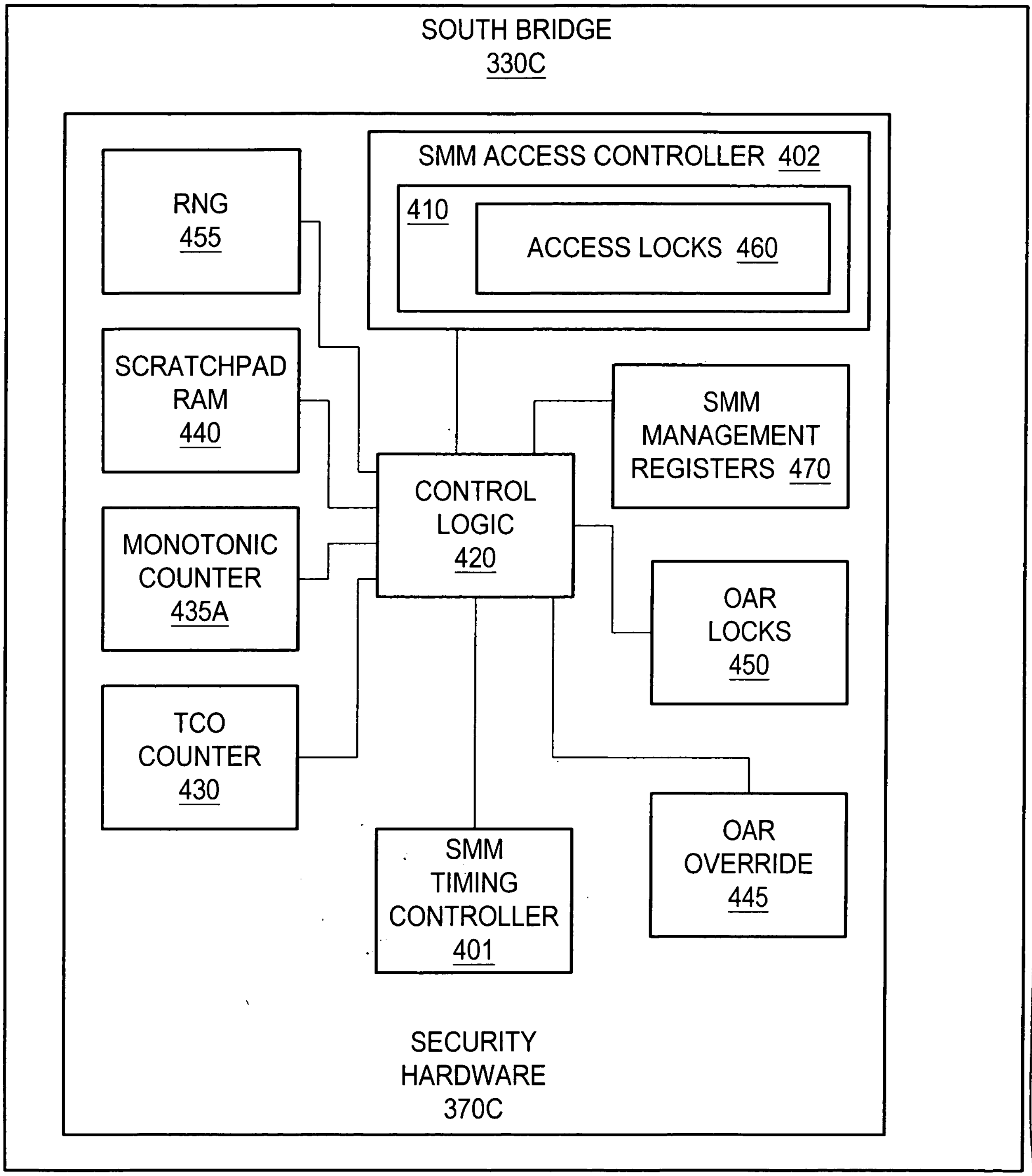

SOUTH BRIDGE
330C
SMM ACCESS CONTROLLER 402
410
ACCESS LOCKS 460
RNG
455
SCRATCHPAD
RAM
440
MONOTONIC
COUNTER
435A
TCO
COUNTER
430
CONTROL
LOGIC
420
SMM
MANAGEMENT
REGISTERS 470
OAR
LOCKS
450
SMM
TIMING
CONTROLLER
401
OAR
OVERRIDE
445
SECURITY
HARDWARE
370C

Fig. 6

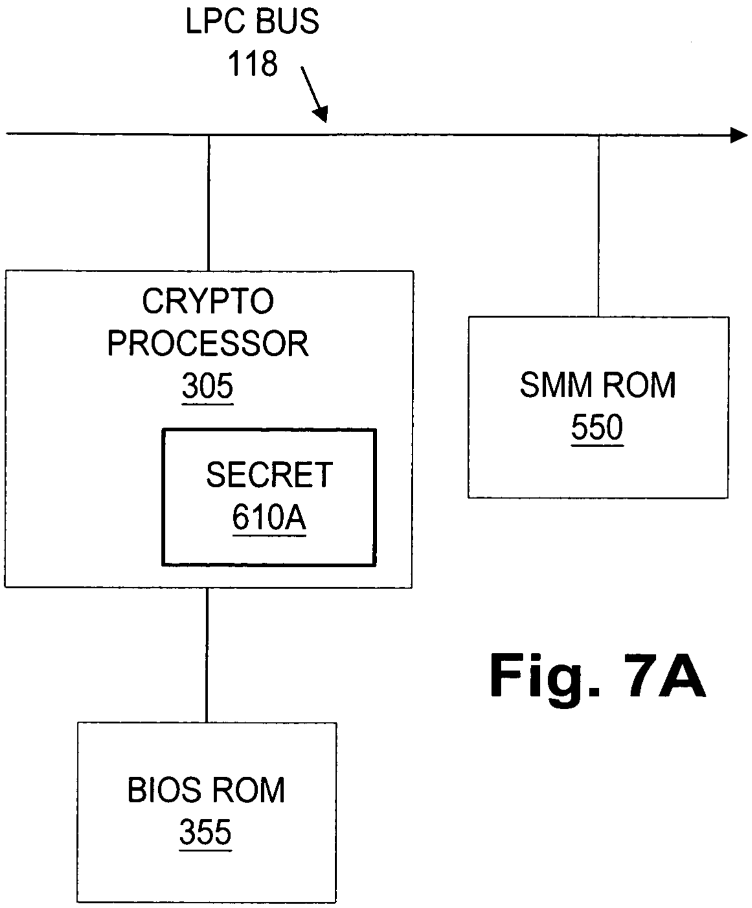

LPC BUS
118
CRYPTO PROCESSOR
305
SECRET
610A
SMM ROM
550
BIOS ROM
355

Fig. 7A

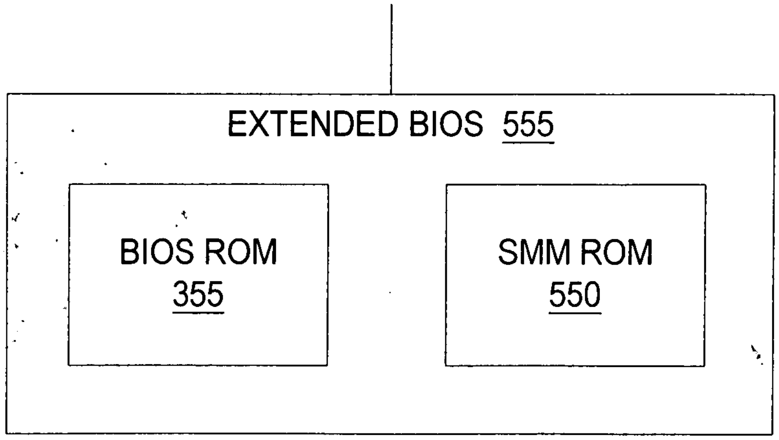

EXTENDED BIOS 555
BIOS ROM
355
SMM ROM
550

Fig. 7B

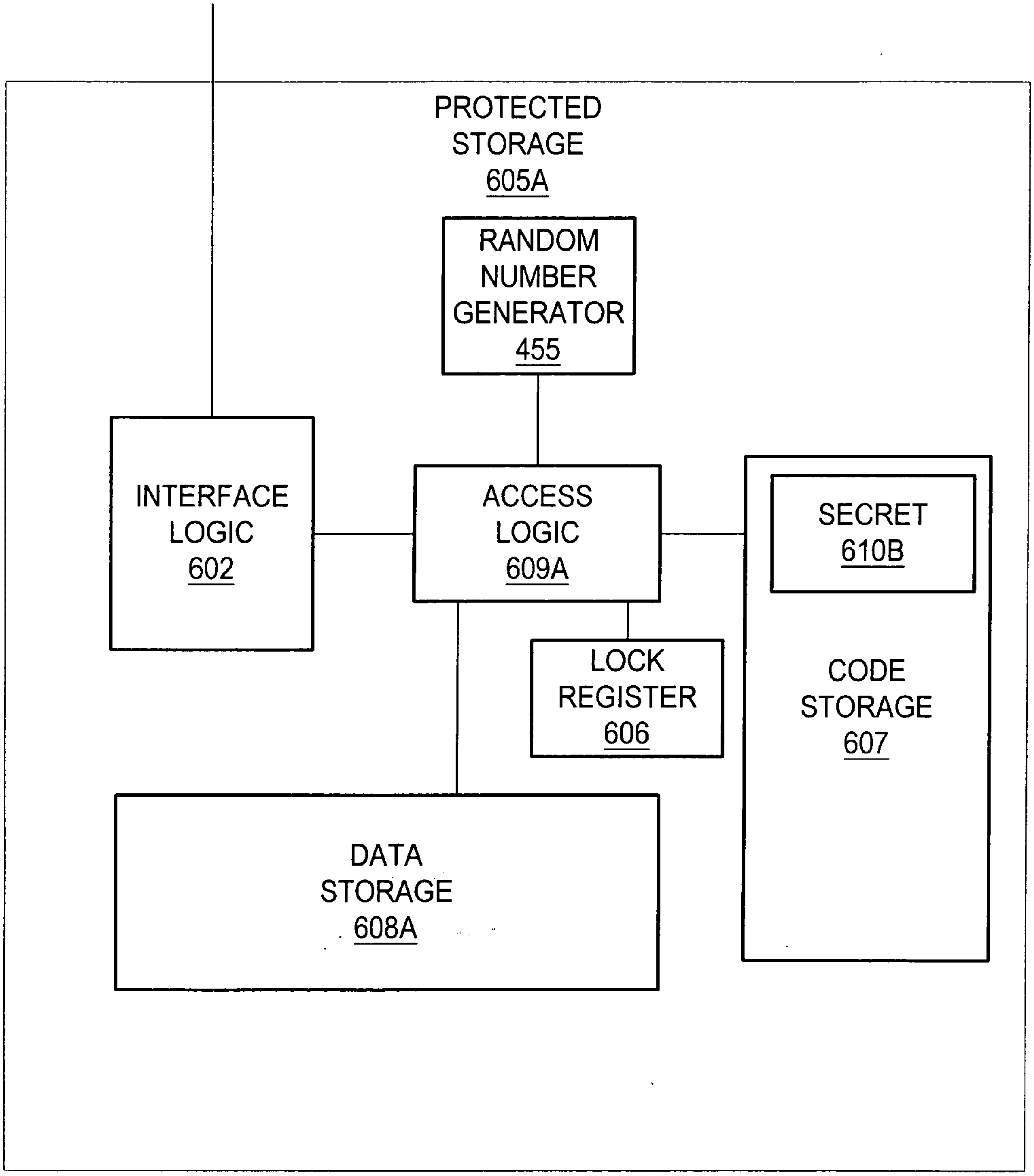

PROTECTED STORAGE 605A
RANDOM NUMBER GENERATOR 455
INTERFACE LOGIC 602
ACCESS LOGIC 609A
SECRET 610B
LOCK REGISTER 606
CODE STORAGE 607
DATA STORAGE 608A

Fig. 7C

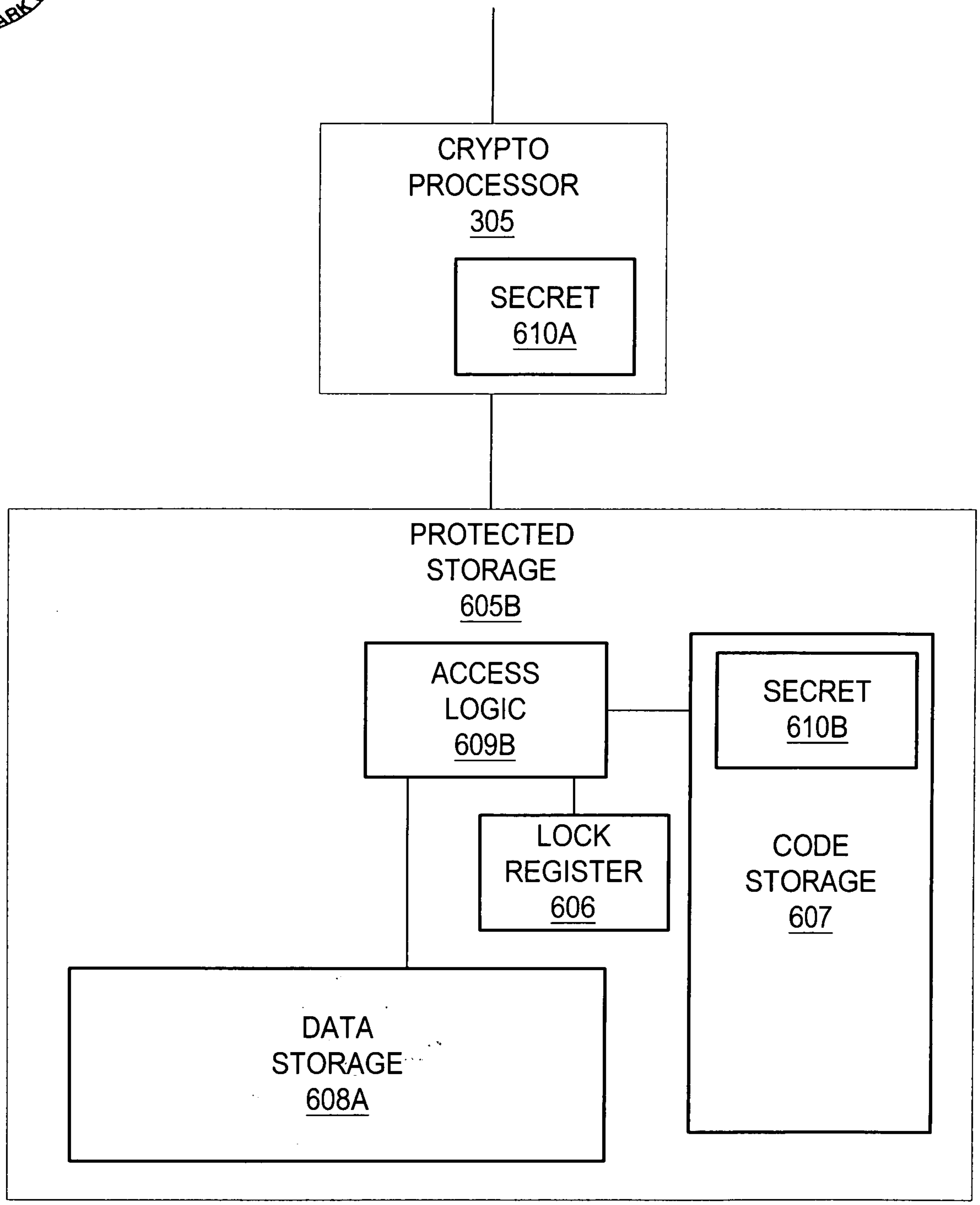

CRYPTO PROCESSOR 305
SECRET 610A
PROTECTED STORAGE 605B
ACCESS LOGIC 609B
SECRET 610B
LOCK REGISTER 606
CODE STORAGE 607
DATA STORAGE 608A

Fig. 7D

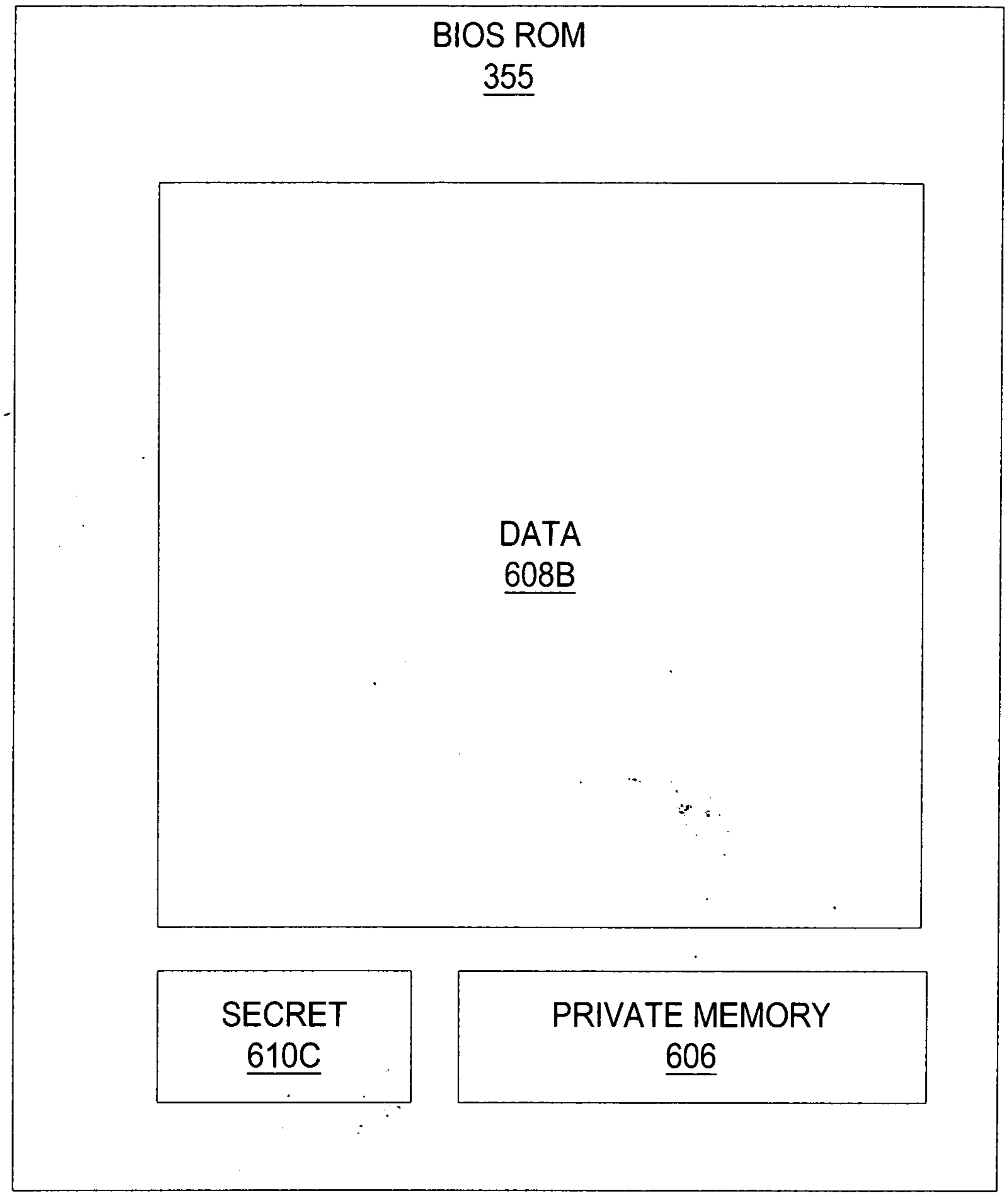


Fig. 8A

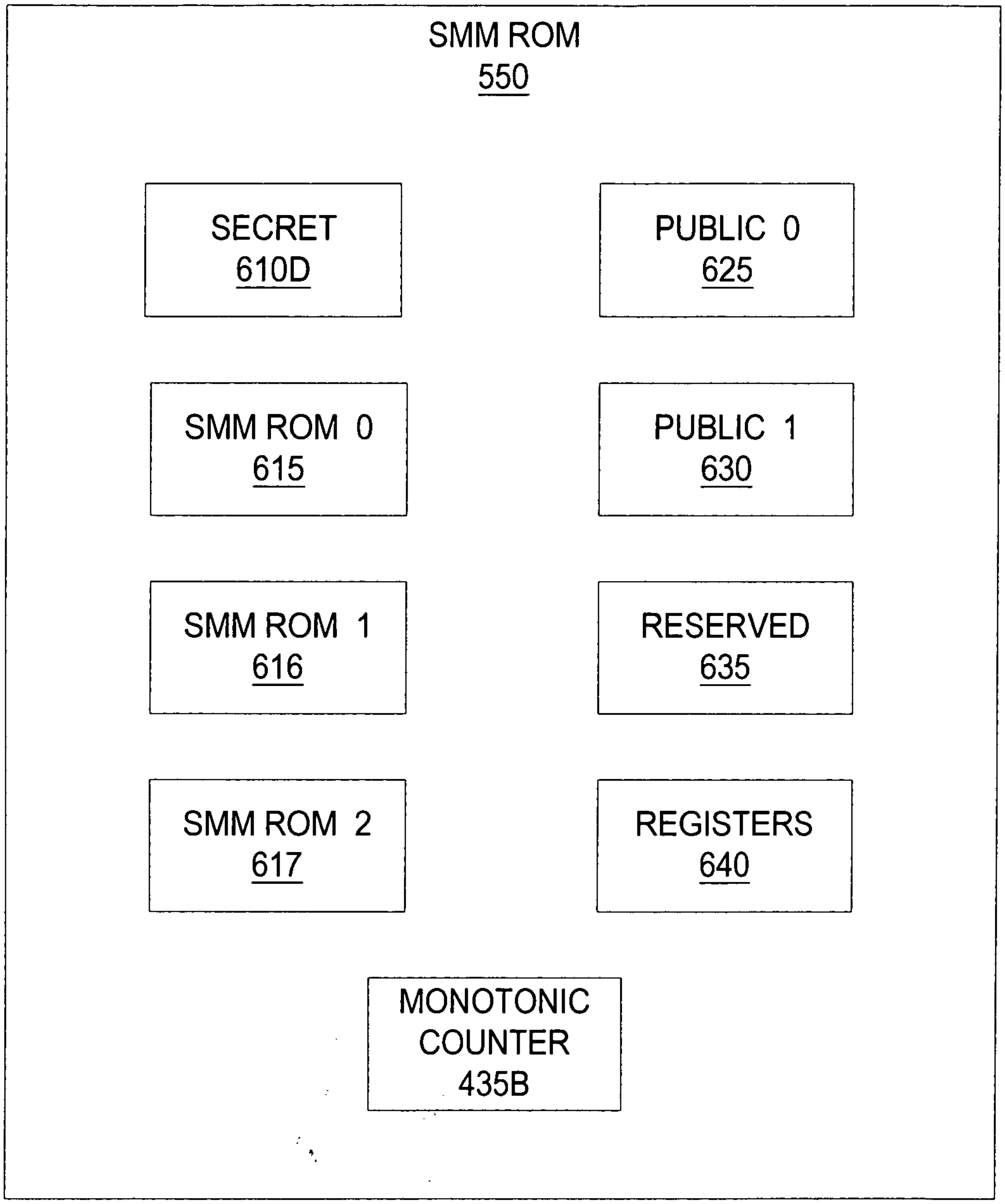

SMM ROM
550
SECRET
610D
PUBLIC 0
625
SMM ROM 0
615
PUBLIC 1
630
SMM ROM 1
616
RESERVED
635
SMM ROM 2
617
REGISTERS
640
MONOTONIC
COUNTER
435B

Fig. 8B

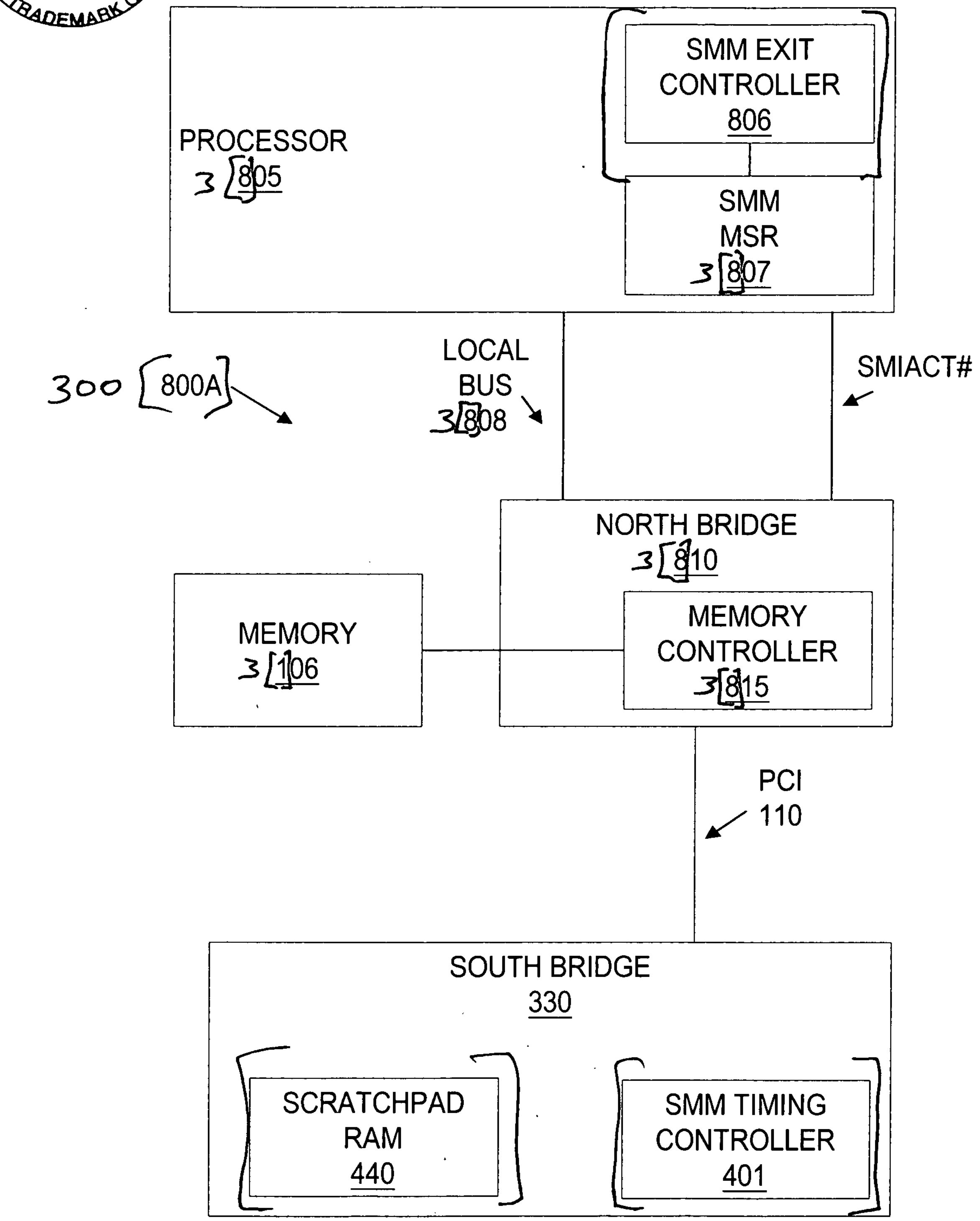

SMM EXIT CONTROLLER
806
PROCESSOR
3 805
SMM MSR
3 807
300 800A
LOCAL BUS
3 808
SMIACT#
NORTH BRIDGE
3 810
MEMORY
3 106
MEMORY CONTROLLER
3 815
PCI
110
SOUTH BRIDGE
330
SCRATCHPAD RAM
440
SMM TIMING CONTROLLER
401

Fig. 9A 3

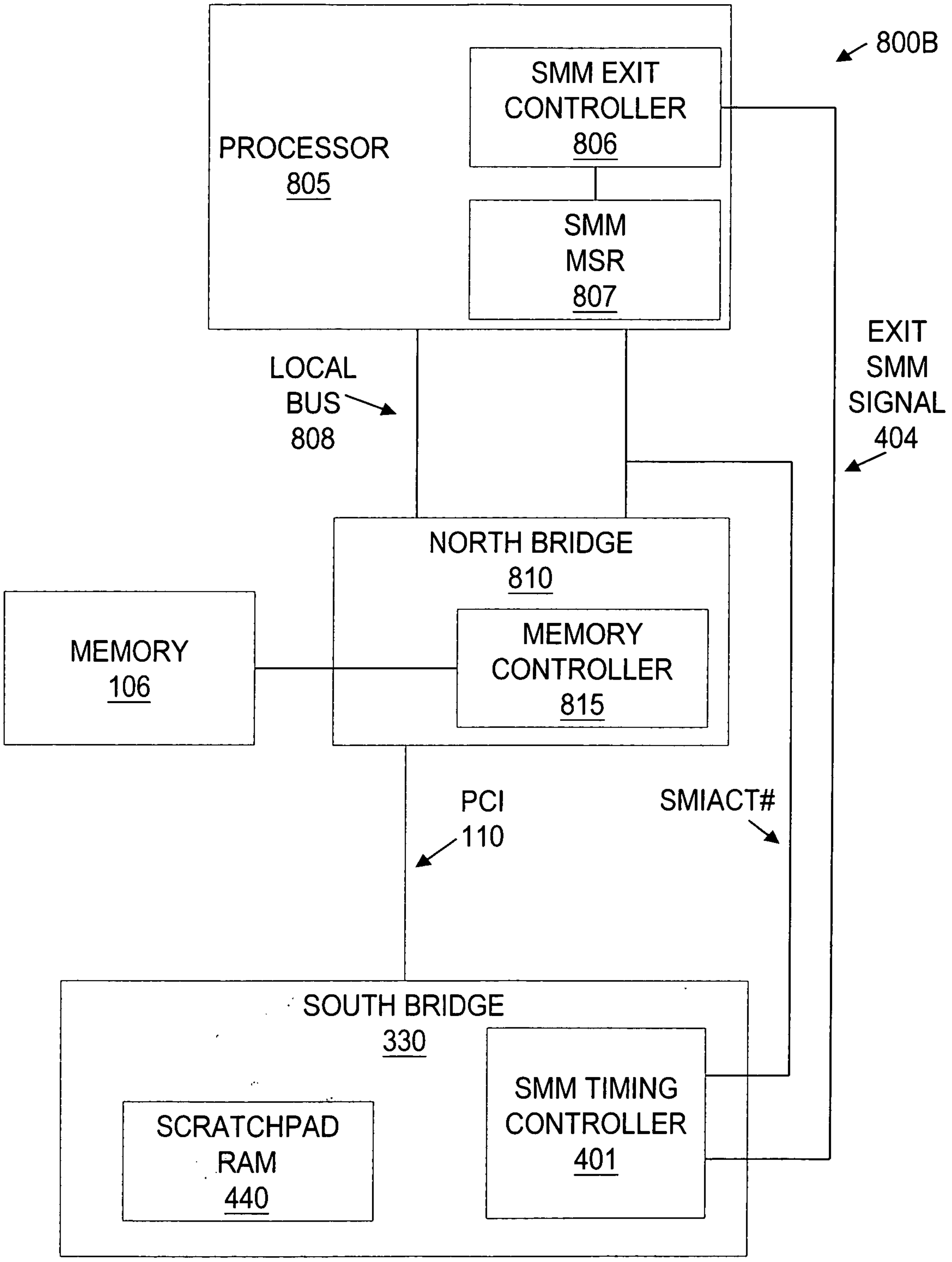

800B
PROCESSOR
805
SMM EXIT
CONTROLLER
806
SMM
MSR
807
LOCAL
BUS
808
EXIT
SMM
SIGNAL
404
NORTH BRIDGE
810
MEMORY
106
MEMORY
CONTROLLER
815
PCI
110
SMIACT#
SOUTH BRIDGE
330
SCRATCHPAD
RAM
440
SMM TIMING
CONTROLLER
401

Fig. 9B

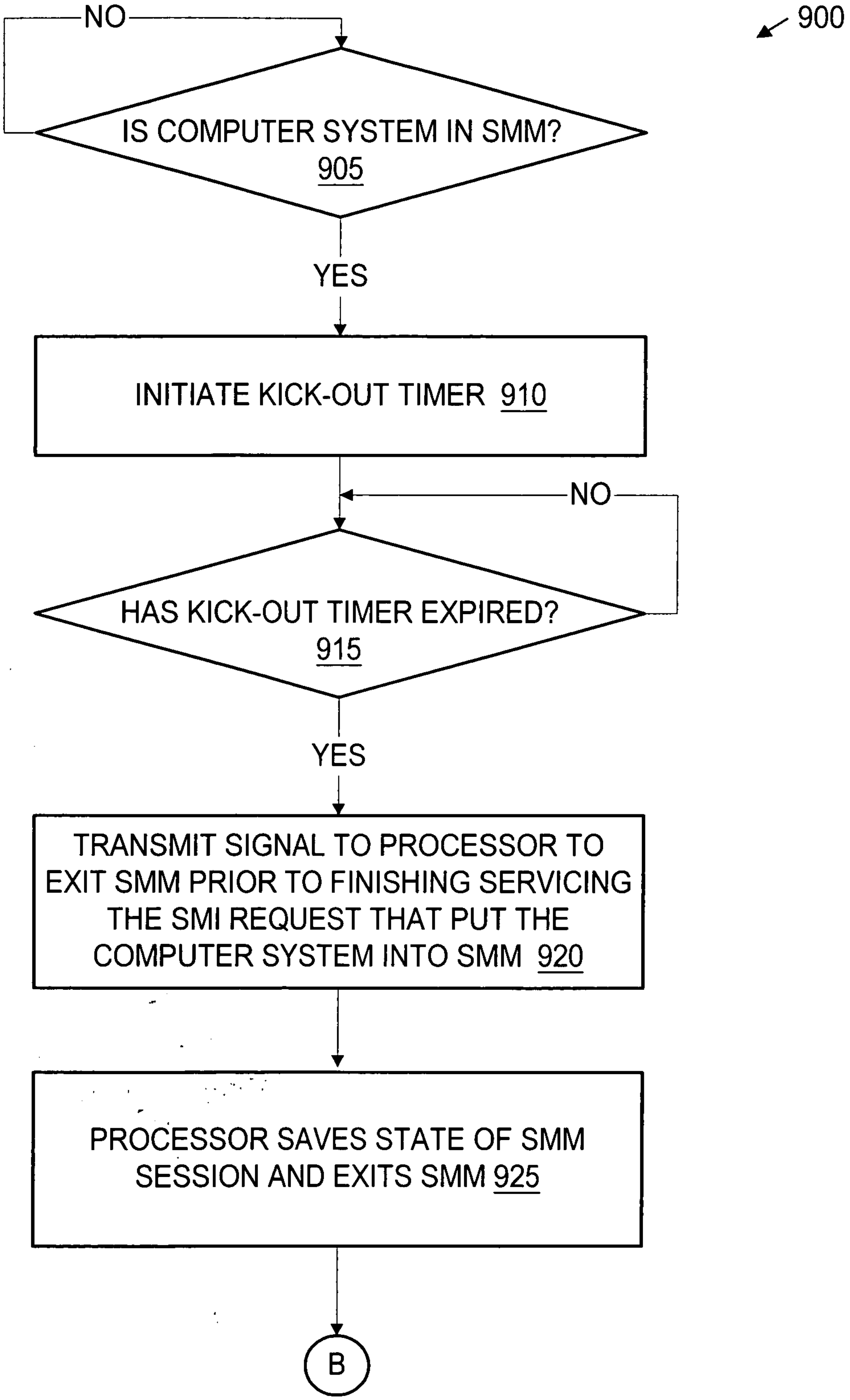

900
NO
IS COMPUTER SYSTEM IN SMM? 905
YES
INITIATE KICK-OUT TIMER 910
NO
HAS KICK-OUT TIMER EXPIRED? 915
YES
TRANSMIT SIGNAL TO PROCESSOR TO EXIT SMM PRIOR TO FINISHING SERVICING THE SMI REQUEST THAT PUT THE COMPUTER SYSTEM INTO SMM 920
PROCESSOR SAVES STATE OF SMM SESSION AND EXITS SMM 925
B

Fig. 10A

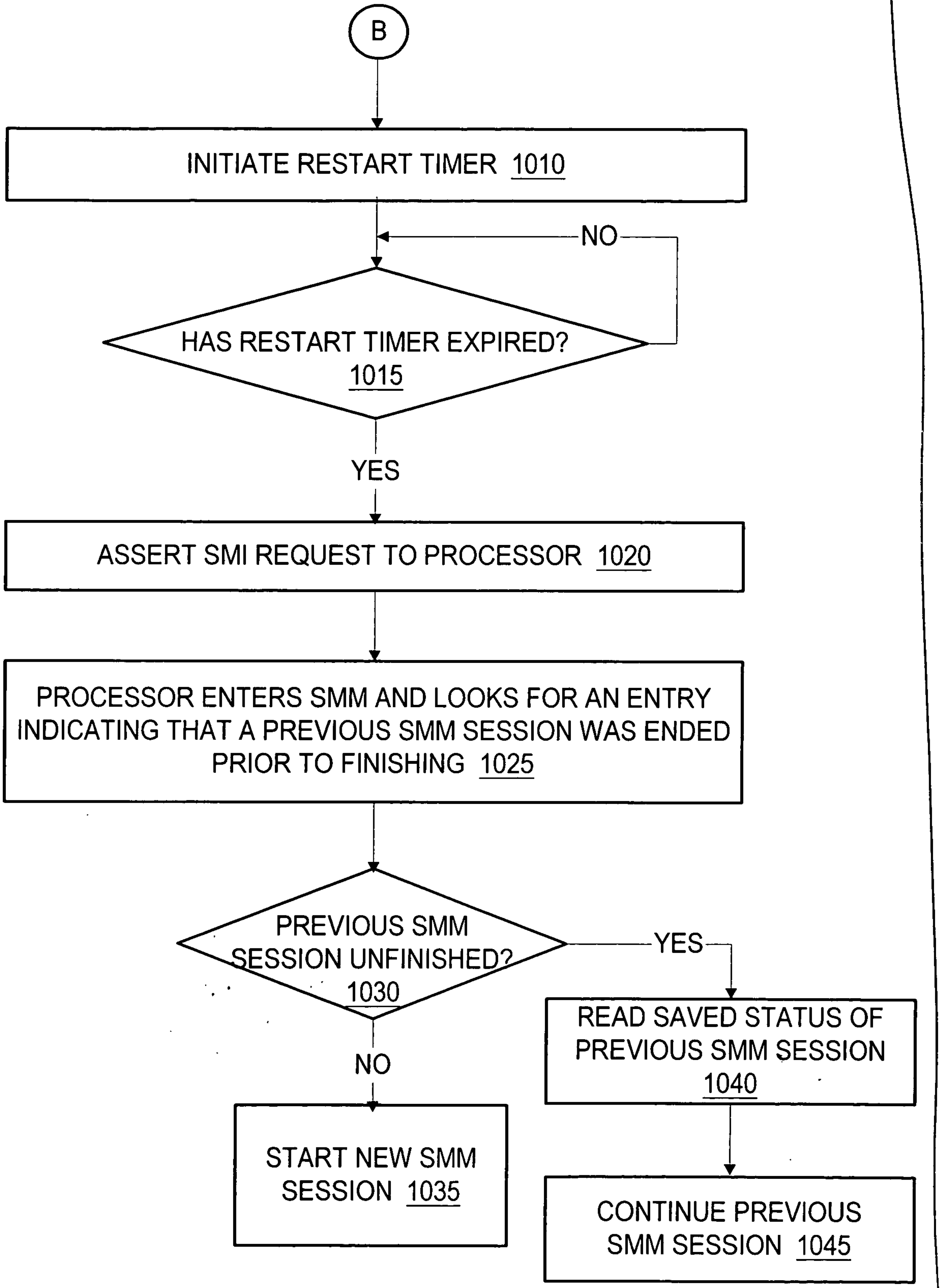

B
INITIATE RESTART TIMER 1010
NO
HAS RESTART TIMER EXPIRED? 1015
YES
ASSERT SMI REQUEST TO PROCESSOR 1020
PROCESSOR ENTERS SMM AND LOOKS FOR AN ENTRY INDICATING THAT A PREVIOUS SMM SESSION WAS ENDED PRIOR TO FINISHING 1025
PREVIOUS SMM SESSION UNFINISHED? 1030
YES
READ SAVED STATUS OF PREVIOUS SMM SESSION 1040
NO
START NEW SMM SESSION 1035
CONTINUE PREVIOUS SMM SESSION 1045

Fig. 10B

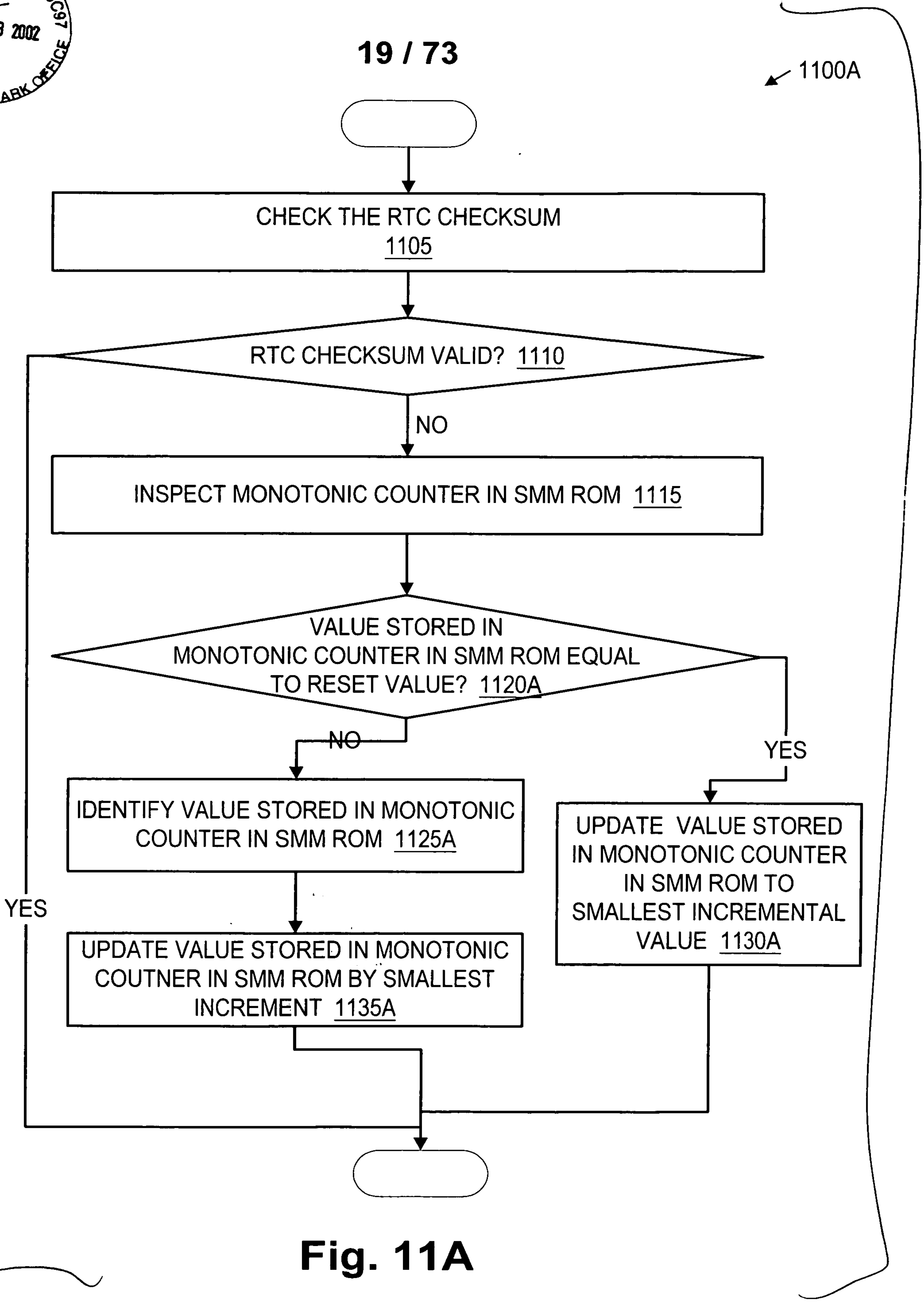

1100A
CHECK THE RTC CHECKSUM 1105
RTC CHECKSUM VALID? 1110
NO
INSPECT MONOTONIC COUNTER IN SMM ROM 1115
VALUE STORED IN MONOTONIC COUNTER IN SMM ROM EQUAL TO RESET VALUE? 1120A
NO
YES
IDENTIFY VALUE STORED IN MONOTONIC COUNTER IN SMM ROM 1125A
UPDATE VALUE STORED IN MONOTONIC COUNTER IN SMM ROM TO SMALLEST INCREMENTAL VALUE 1130A
YES
UPDATE VALUE STORED IN MONOTONIC COUTNER IN SMM ROM BY SMALLEST INCREMENT 1135A

Fig. 11A

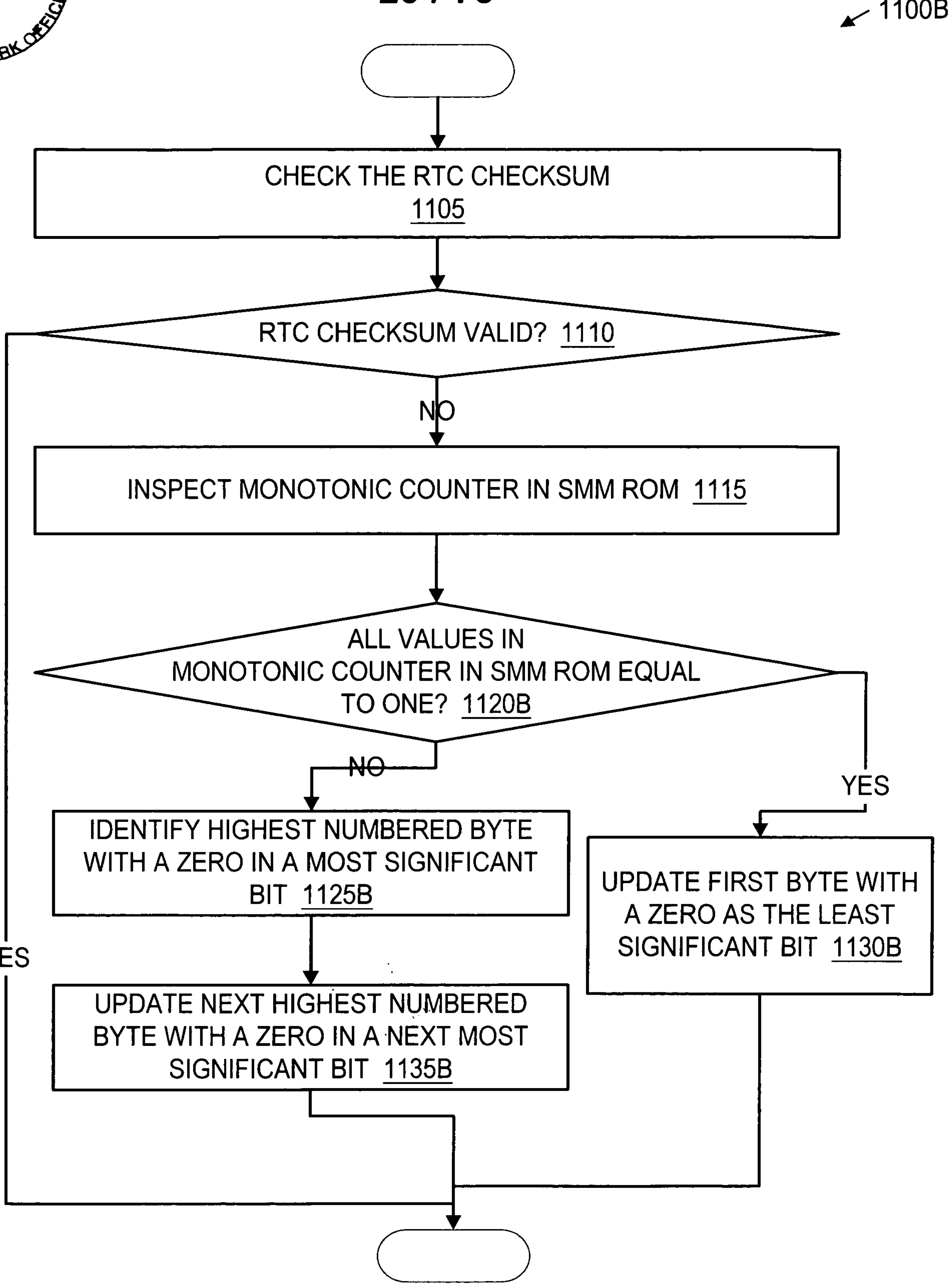

1100B
CHECK THE RTC CHECKSUM 1105
RTC CHECKSUM VALID? 1110
NO
YES
INSPECT MONOTONIC COUNTER IN SMM ROM 1115
ALL VALUES IN MONOTONIC COUNTER IN SMM ROM EQUAL TO ONE? 1120B
NO
YES
IDENTIFY HIGHEST NUMBERED BYTE WITH A ZERO IN A MOST SIGNIFICANT BIT 1125B
UPDATE NEXT HIGHEST NUMBERED BYTE WITH A ZERO IN A NEXT MOST SIGNIFICANT BIT 1135B
UPDATE FIRST BYTE WITH A ZERO AS THE LEAST SIGNIFICANT BIT 1130B

Fig. 11B

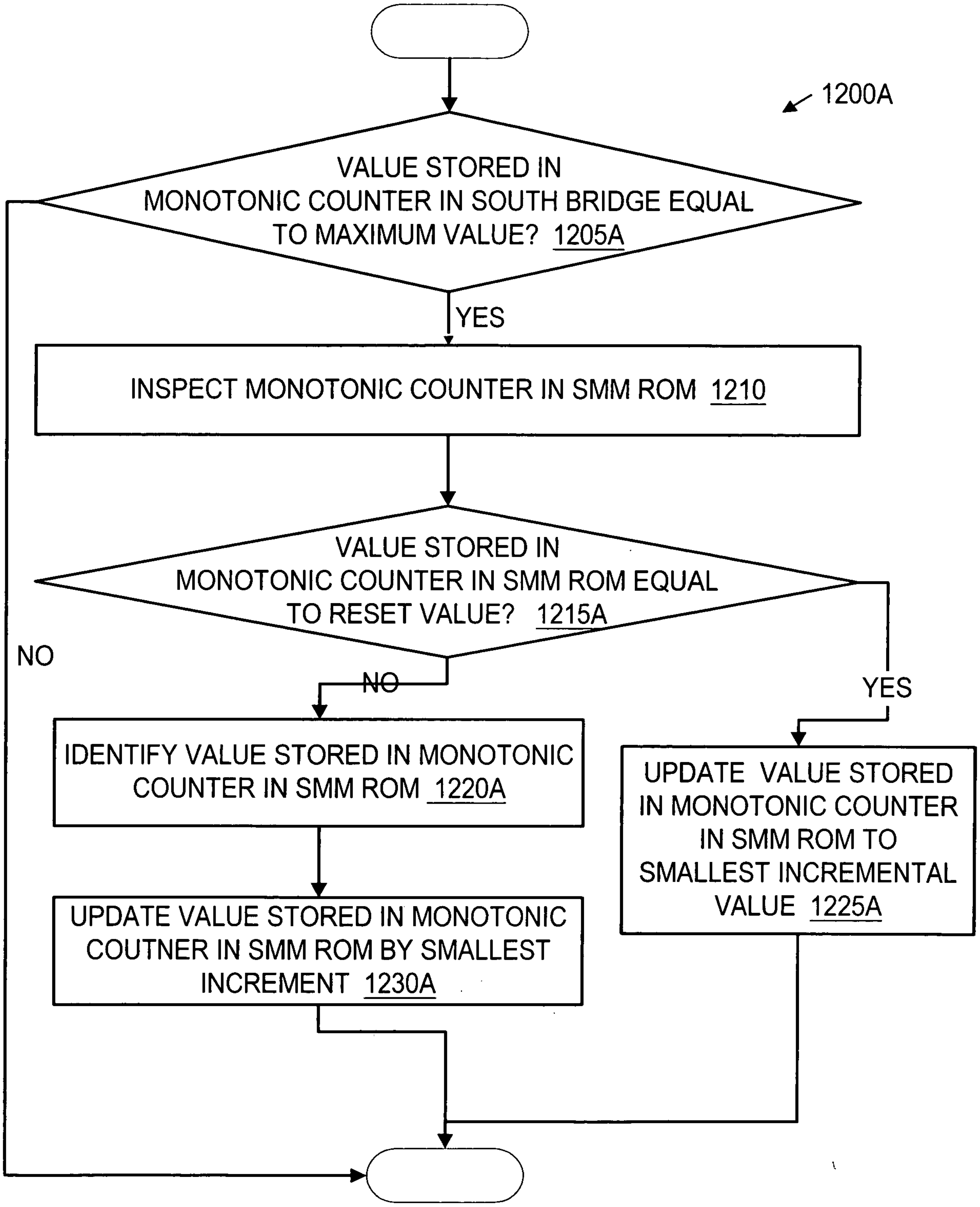

1200A
VALUE STORED IN MONOTONIC COUNTER IN SOUTH BRIDGE EQUAL TO MAXIMUM VALUE? 1205A
YES
NO
INSPECT MONOTONIC COUNTER IN SMM ROM 1210
VALUE STORED IN MONOTONIC COUNTER IN SMM ROM EQUAL TO RESET VALUE? 1215A
NO
YES
IDENTIFY VALUE STORED IN MONOTONIC COUNTER IN SMM ROM 1220A
UPDATE VALUE STORED IN MONOTONIC COUTNER IN SMM ROM BY SMALLEST INCREMENT 1230A
UPDATE VALUE STORED IN MONOTONIC COUNTER IN SMM ROM TO SMALLEST INCREMENTAL VALUE 1225A

Fig. 12A

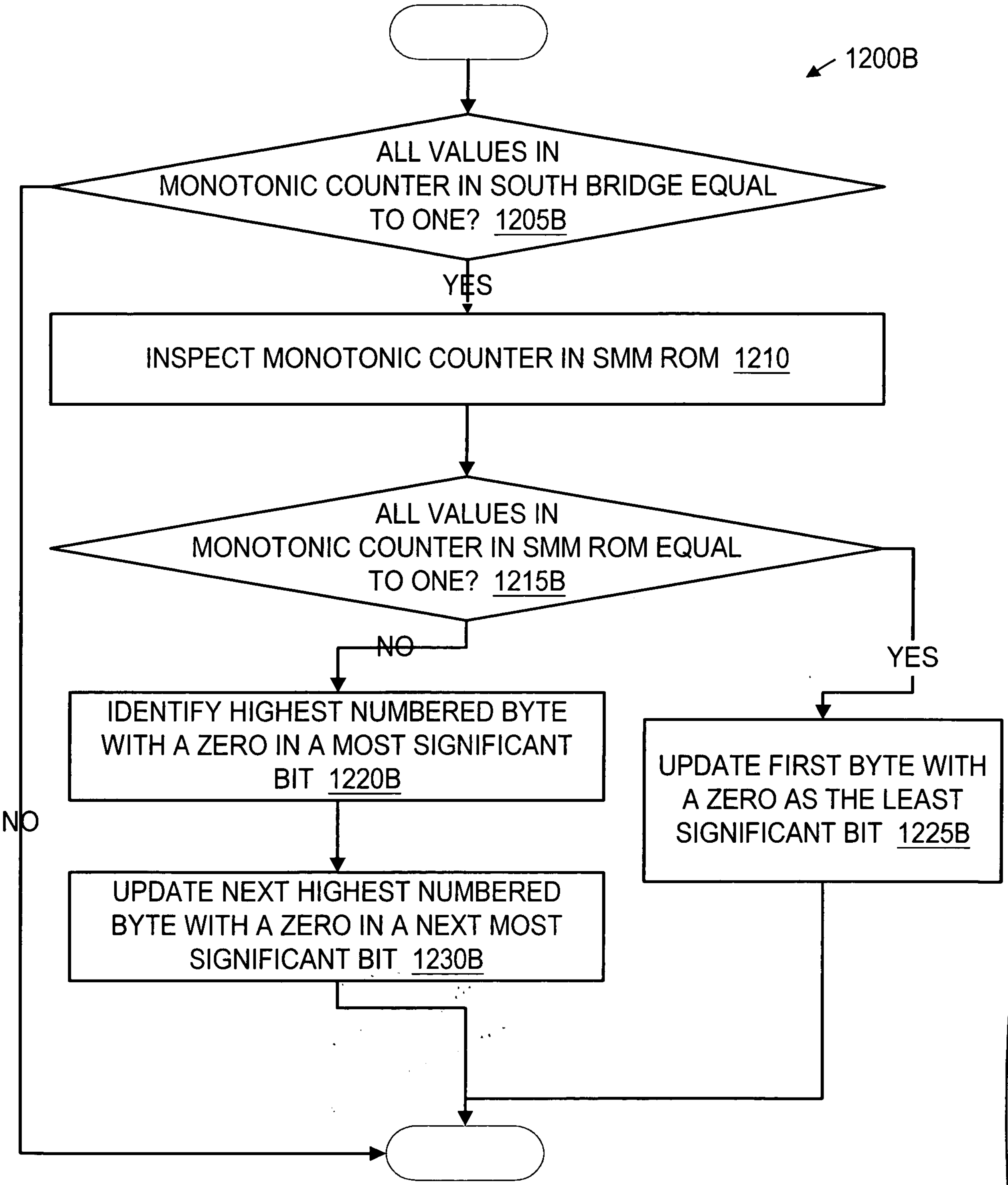

1200B
ALL VALUES IN MONOTONIC COUNTER IN SOUTH BRIDGE EQUAL TO ONE? 1205B
YES
NO
INSPECT MONOTONIC COUNTER IN SMM ROM 1210
ALL VALUES IN MONOTONIC COUNTER IN SMM ROM EQUAL TO ONE? 1215B
NO
YES
IDENTIFY HIGHEST NUMBERED BYTE WITH A ZERO IN A MOST SIGNIFICANT BIT 1220B
UPDATE FIRST BYTE WITH A ZERO AS THE LEAST SIGNIFICANT BIT 1225B
UPDATE NEXT HIGHEST NUMBERED BYTE WITH A ZERO IN A NEXT MOST SIGNIFICANT BIT 1230B

Fig. 12B

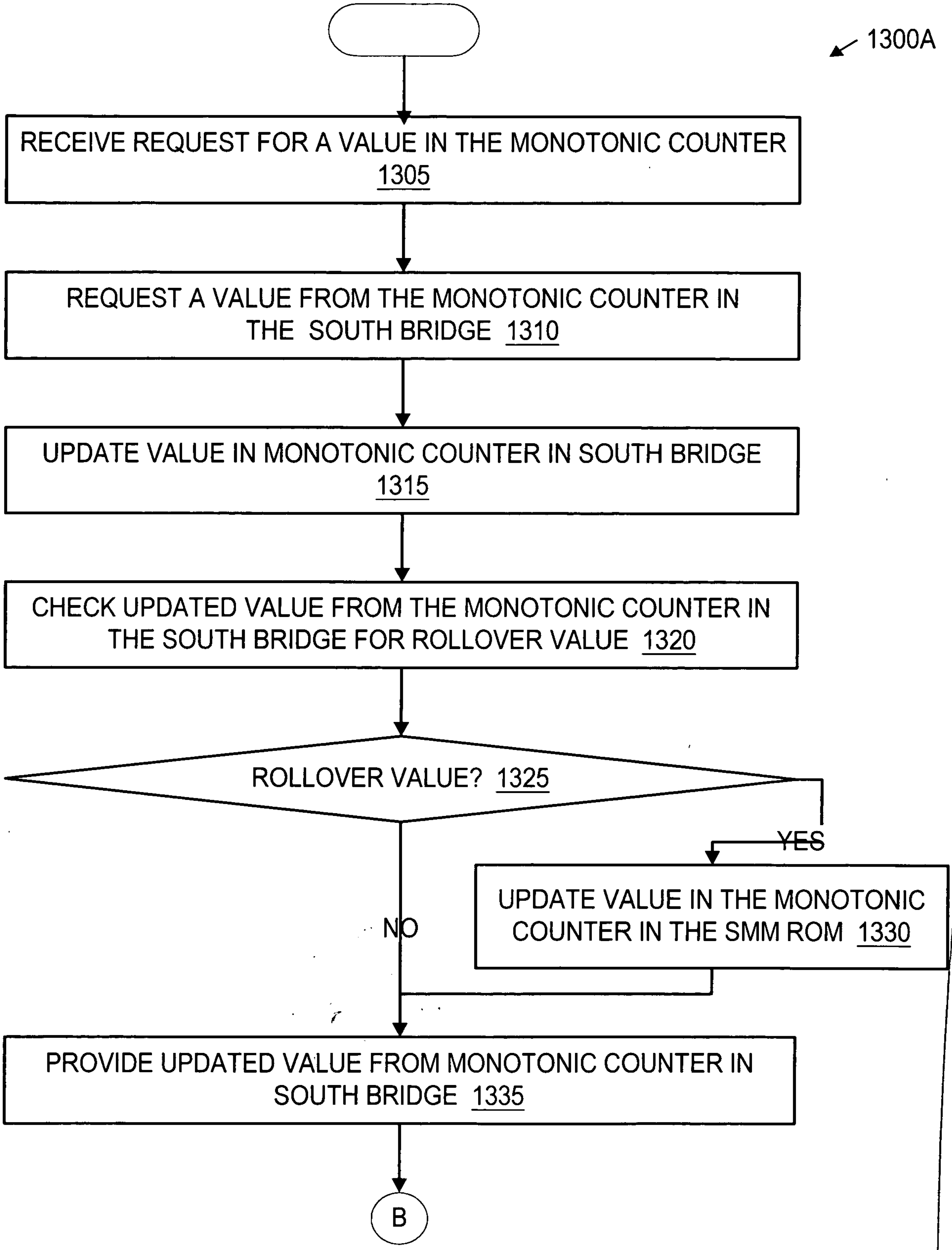

1300A
RECEIVE REQUEST FOR A VALUE IN THE MONOTONIC COUNTER 1305
REQUEST A VALUE FROM THE MONOTONIC COUNTER IN THE SOUTH BRIDGE 1310
UPDATE VALUE IN MONOTONIC COUNTER IN SOUTH BRIDGE 1315
CHECK UPDATED VALUE FROM THE MONOTONIC COUNTER IN THE SOUTH BRIDGE FOR ROLLOVER VALUE 1320
ROLLOVER VALUE? 1325
YES
UPDATE VALUE IN THE MONOTONIC COUNTER IN THE SMM ROM 1330
NO
PROVIDE UPDATED VALUE FROM MONOTONIC COUNTER IN SOUTH BRIDGE 1335
B

Fig. 13A

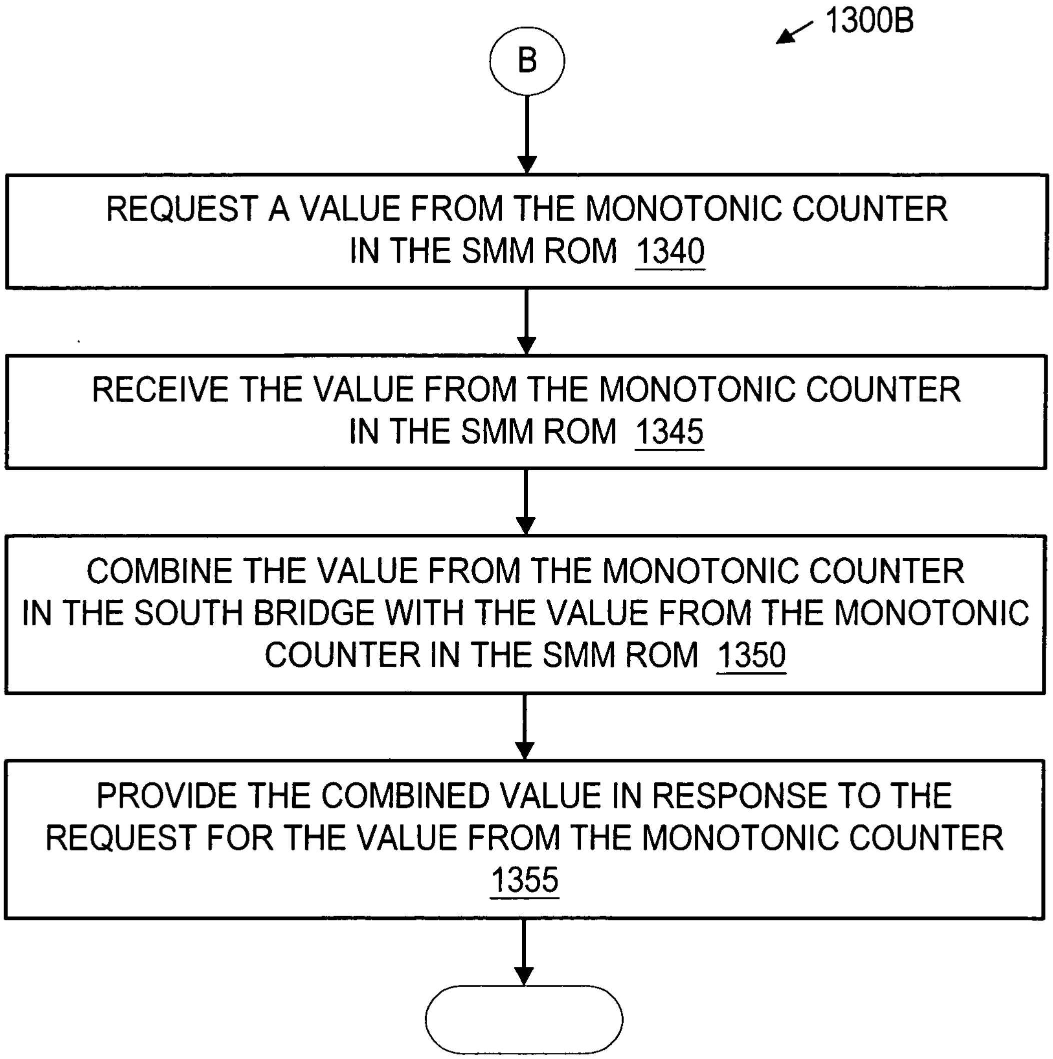

1300B
B
REQUEST A VALUE FROM THE MONOTONIC COUNTER IN THE SMM ROM 1340
RECEIVE THE VALUE FROM THE MONOTONIC COUNTER IN THE SMM ROM 1345
COMBINE THE VALUE FROM THE MONOTONIC COUNTER IN THE SOUTH BRIDGE WITH THE VALUE FROM THE MONOTONIC COUNTER IN THE SMM ROM 1350
PROVIDE THE COMBINED VALUE IN RESPONSE TO THE REQUEST FOR THE VALUE FROM THE MONOTONIC COUNTER 1355

Fig. 13B

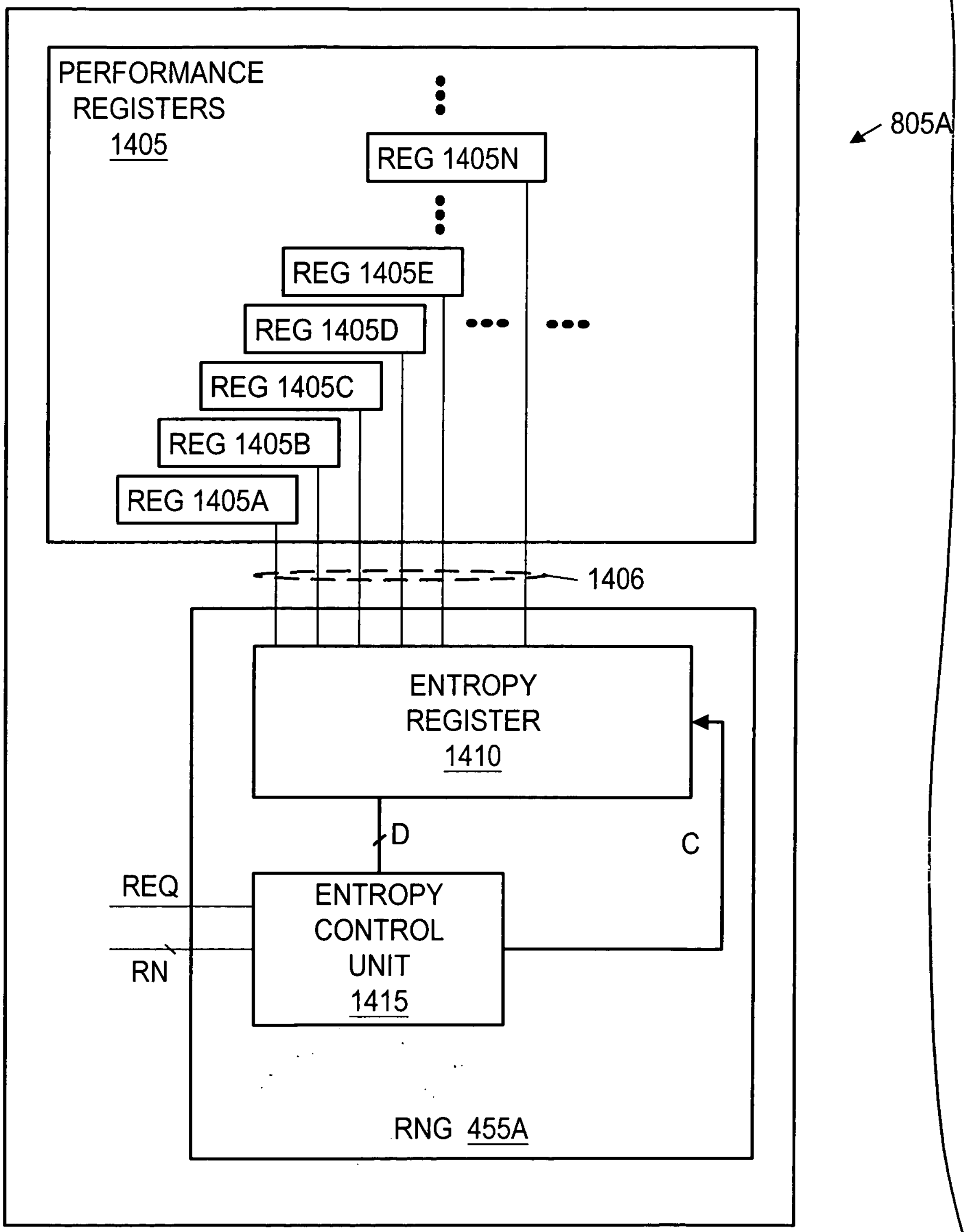

805A
PERFORMANCE REGISTERS
1405
REG 1405N
REG 1405E
REG 1405D
REG 1405C
REG 1405B
REG 1405A
1406
ENTROPY REGISTER
1410
D
C
REQ
RN
ENTROPY CONTROL UNIT
1415
RNG 455A

Fig. 14A

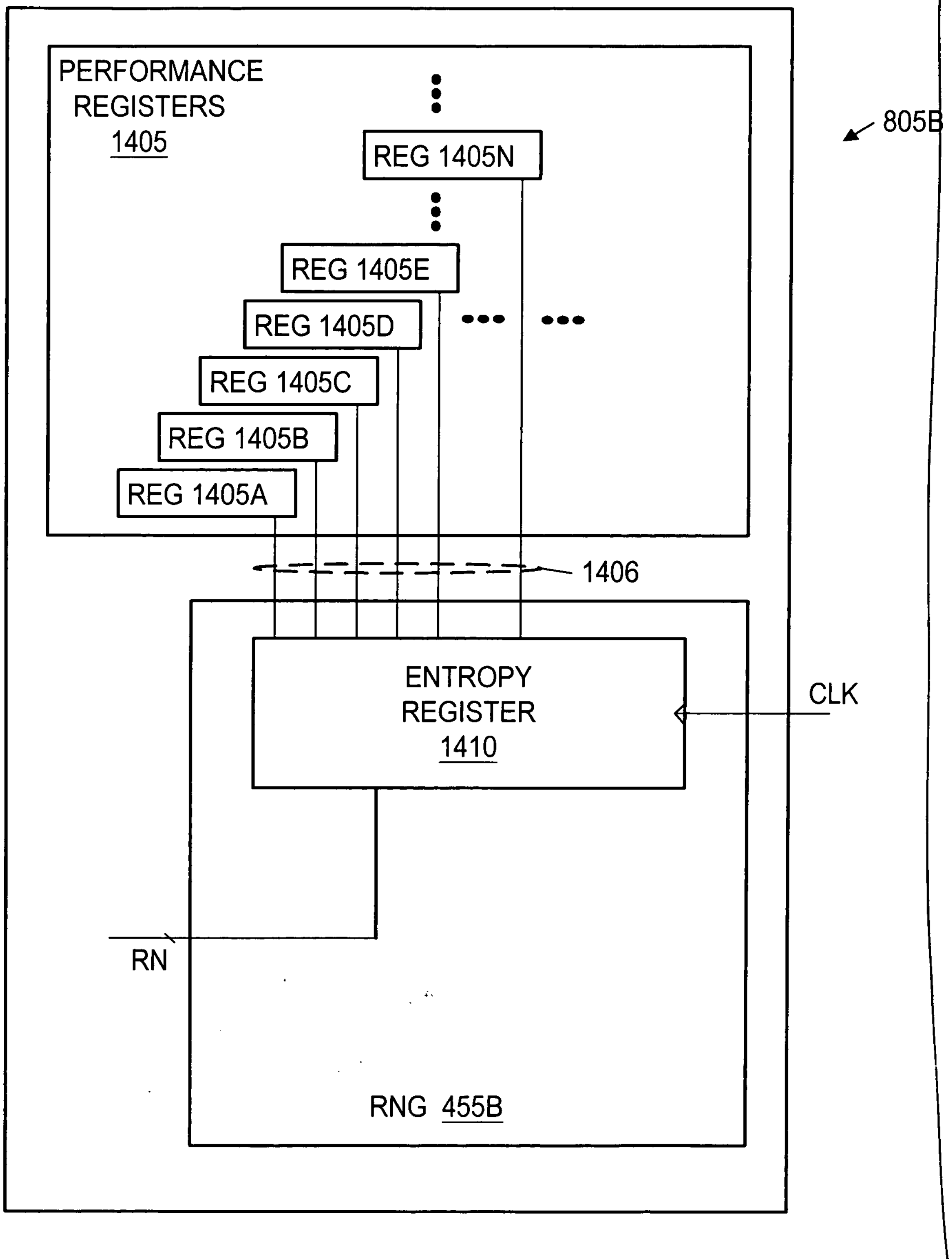

PERFORMANCE REGISTERS 1405
REG 1405N
REG 1405E
REG 1405D
REG 1405C
REG 1405B
REG 1405A
805B
1406
ENTROPY REGISTER 1410
CLK
RN
RNG 455B

Fig. 14B

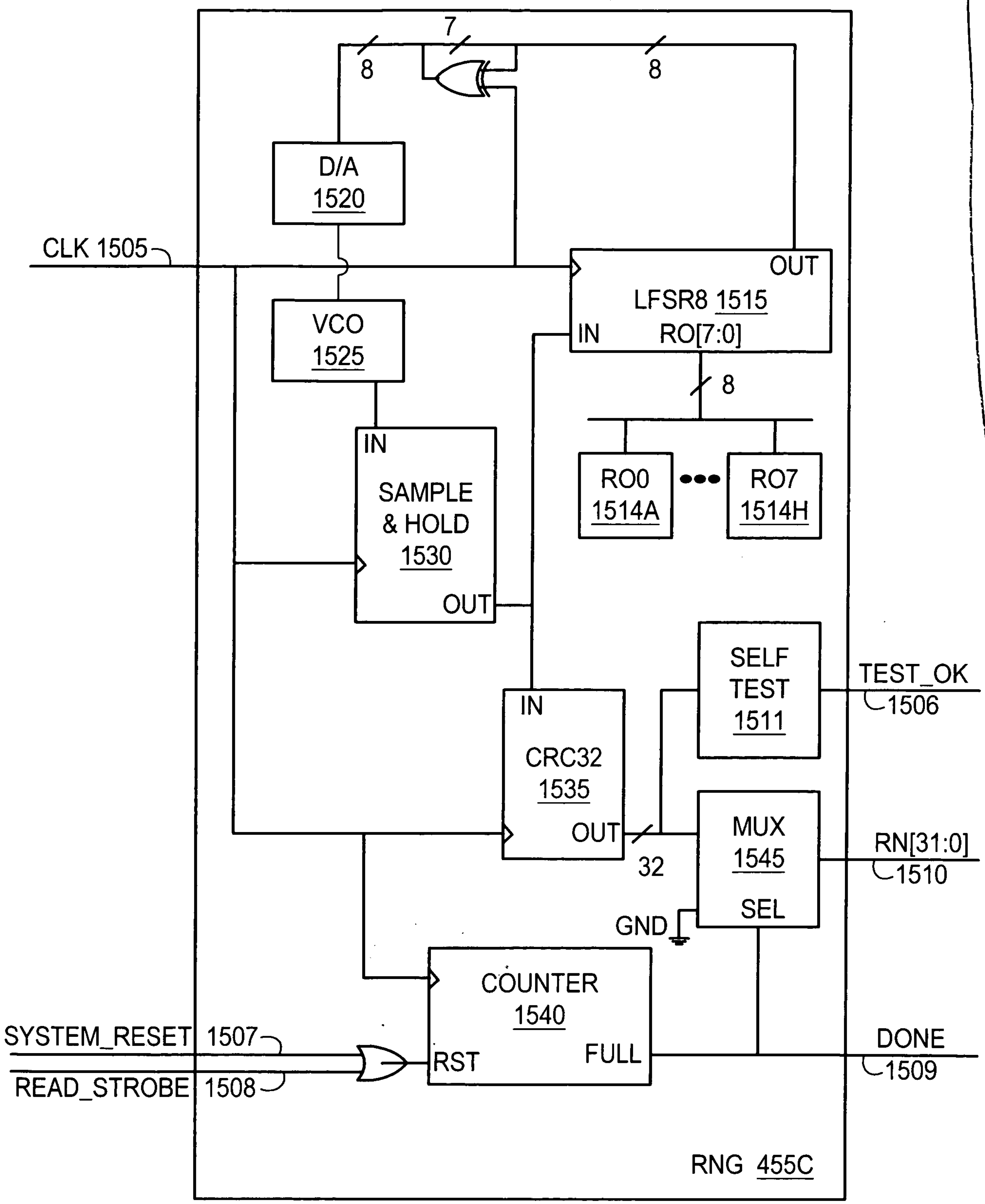

7
8
8
D/A
1520
CLK 1505
OUT
LFSR8 1515
IN
RO[7:0]
VCO
1525
8
IN
SAMPLE
& HOLD
1530
OUT
RO0
1514A
RO7
1514H
SELF
TEST
1511
TEST_OK
1506
IN
CRC32
1535
OUT
32
MUX
1545
SEL
RN[31:0]
1510
GND
COUNTER
1540
RST
FULL
SYSTEM_RESET 1507
READ_STROBE 1508
DONE
1509
RNG 455C

Fig. 15

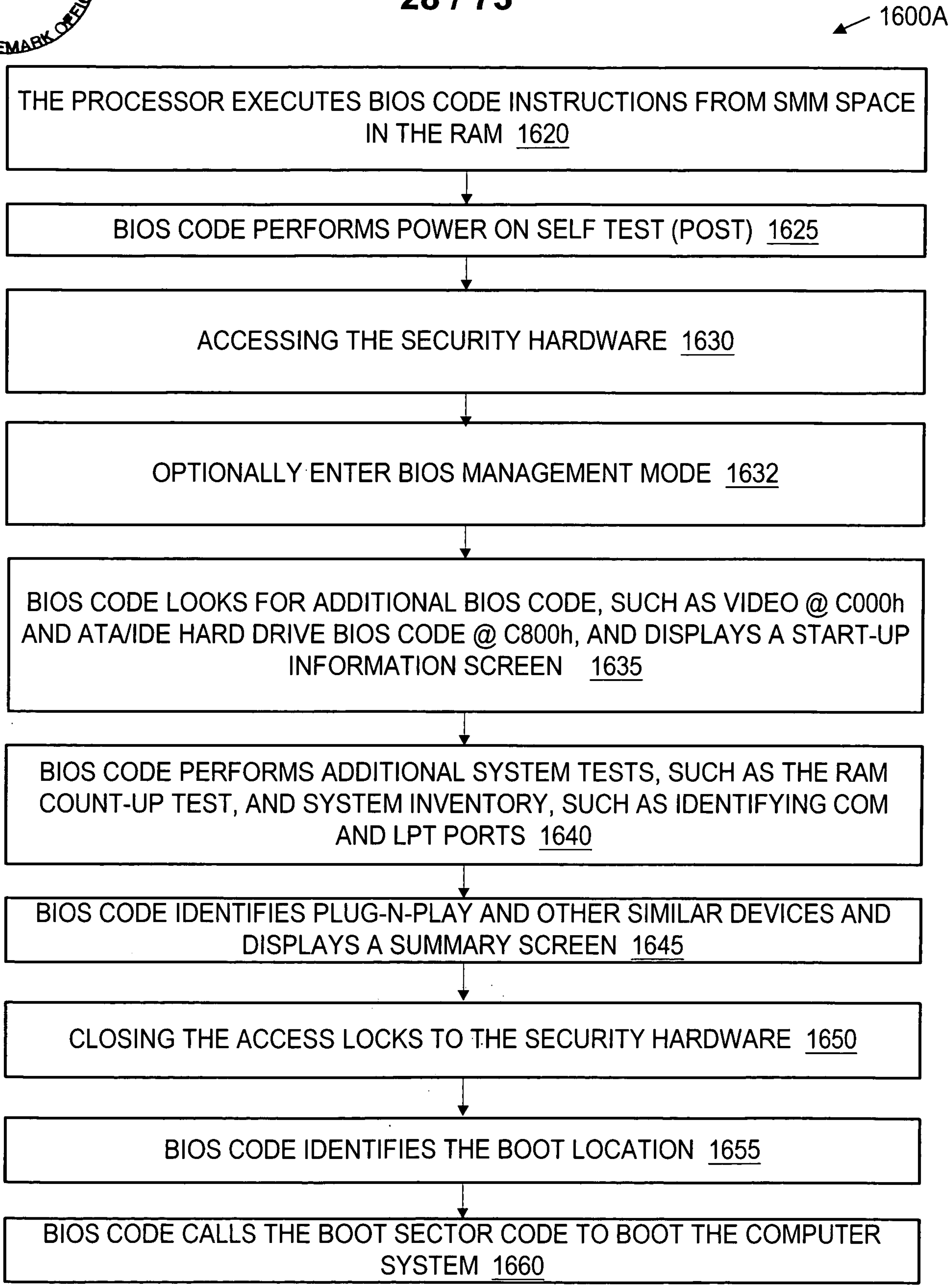

1600A
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620
BIOS CODE PERFORMS POWER ON SELF TEST (POST) 1625
ACCESSING THE SECURITY HARDWARE 1630
OPTIONALLY ENTER BIOS MANAGEMENT MODE 1632
BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 1635
BIOS CODE PERFORMS ADDITIONAL SYSTEM TESTS, SUCH AS THE RAM COUNT-UP TEST, AND SYSTEM INVENTORY, SUCH AS IDENTIFYING COM AND LPT PORTS 1640
BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 1645
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650
BIOS CODE IDENTIFIES THE BOOT LOCATION 1655
BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 1660

Fig. 16A

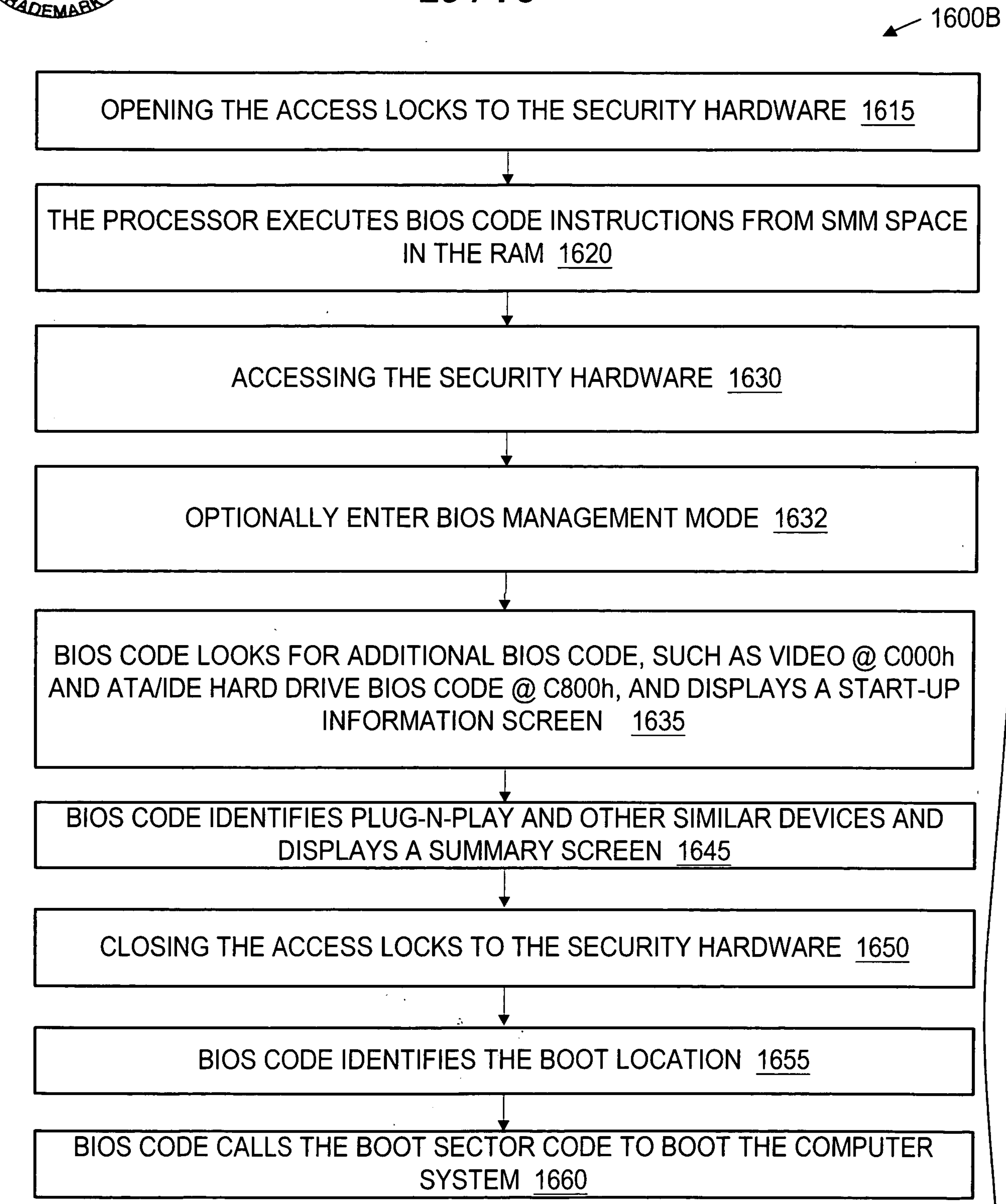

1600B
OPENING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1615
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620
ACCESSING THE SECURITY HARDWARE 1630
OPTIONALLY ENTER BIOS MANAGEMENT MODE 1632
BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 1635
BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 1645
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650
BIOS CODE IDENTIFIES THE BOOT LOCATION 1655
BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 1660

Fig. 16B

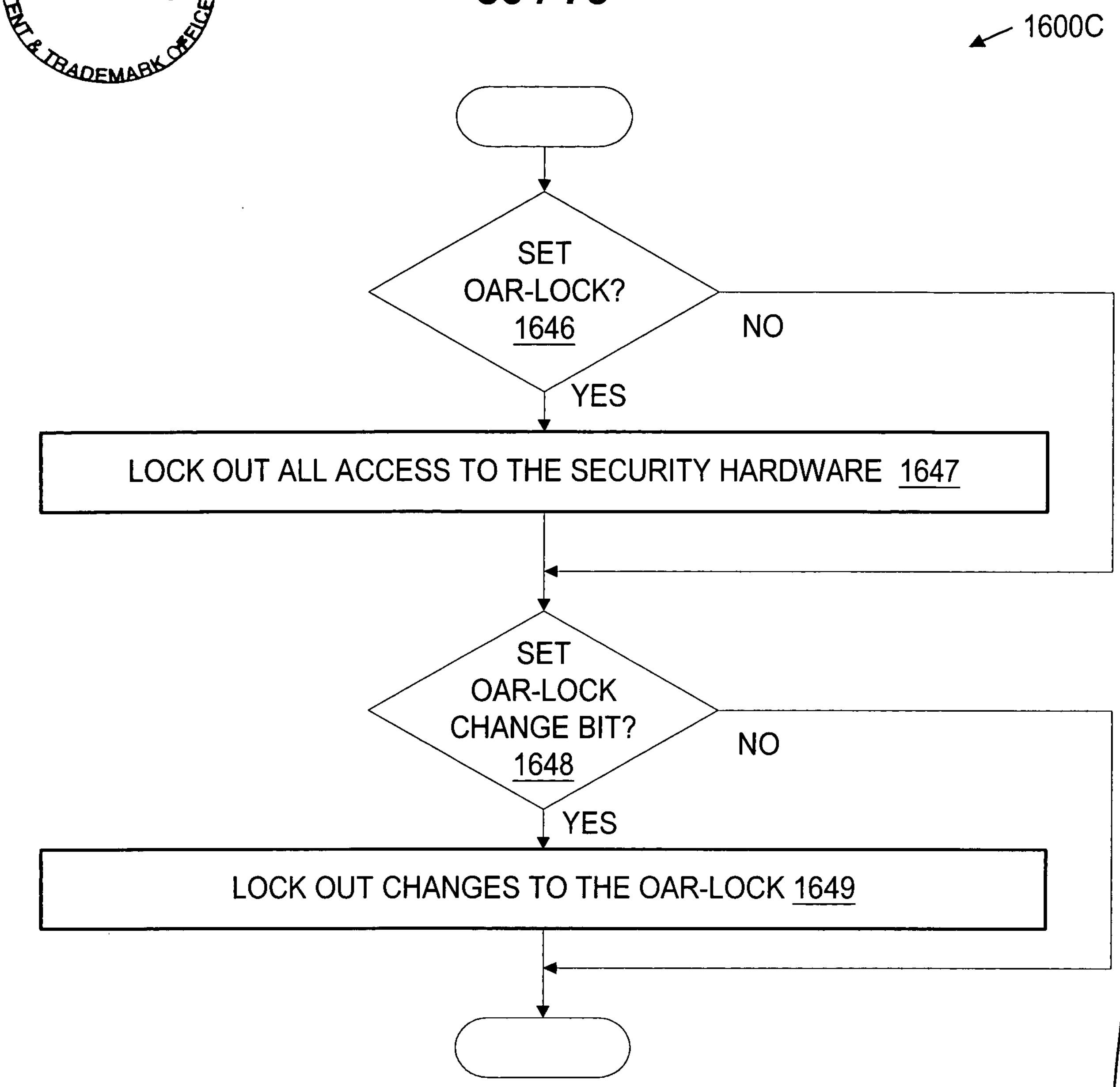

1600C
SET OAR-LOCK? 1646
NO
YES
LOCK OUT ALL ACCESS TO THE SECURITY HARDWARE 1647
SET OAR-LOCK CHANGE BIT? 1648
NO
YES
LOCK OUT CHANGES TO THE OAR-LOCK 1649

Fig. 16C

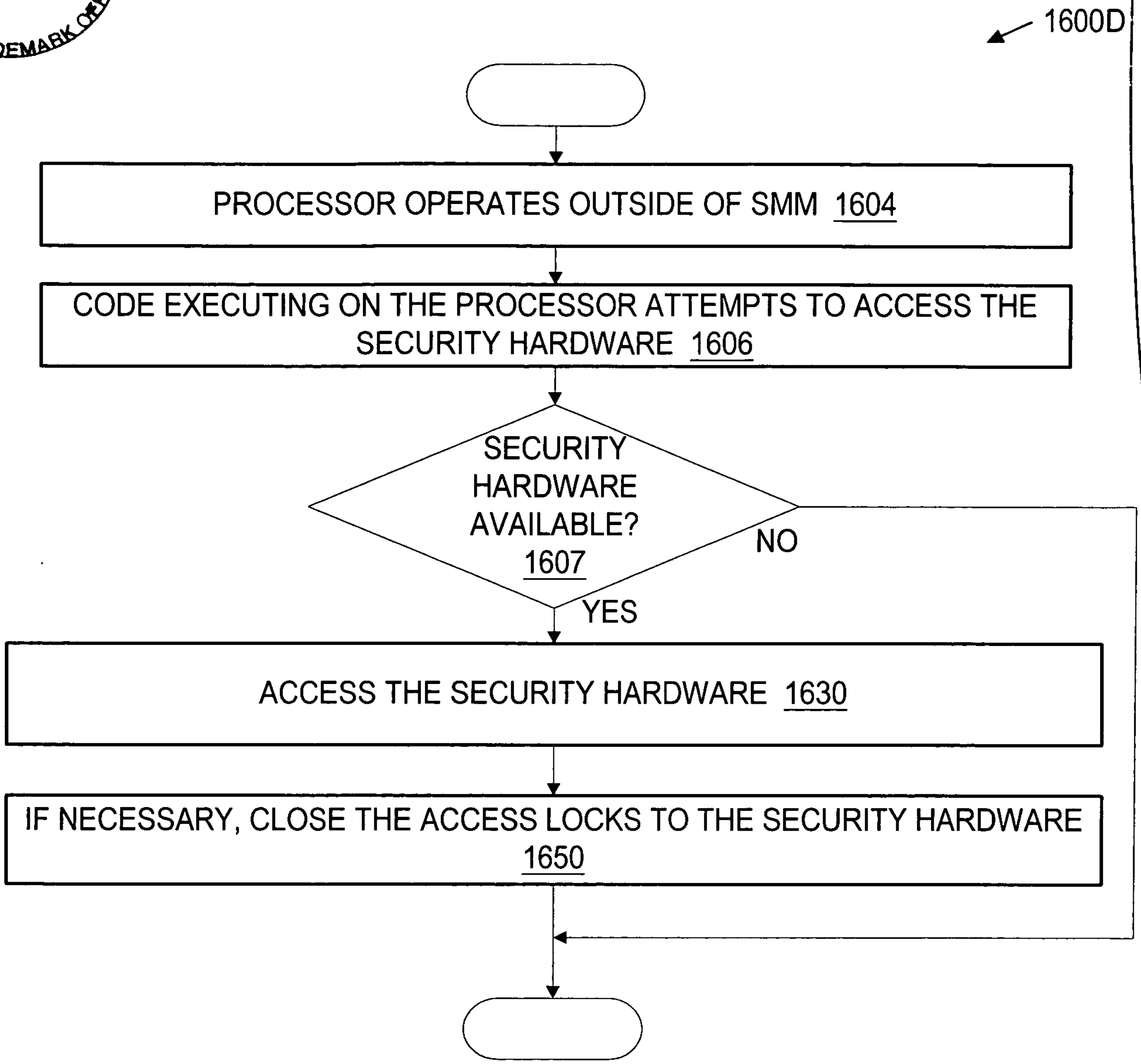

1600D
PROCESSOR OPERATES OUTSIDE OF SMM 1604
CODE EXECUTING ON THE PROCESSOR ATTEMPTS TO ACCESS THE SECURITY HARDWARE 1606
SECURITY HARDWARE AVAILABLE? 1607
NO
YES
ACCESS THE SECURITY HARDWARE 1630
IF NECESSARY, CLOSE THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650

Fig. 16D

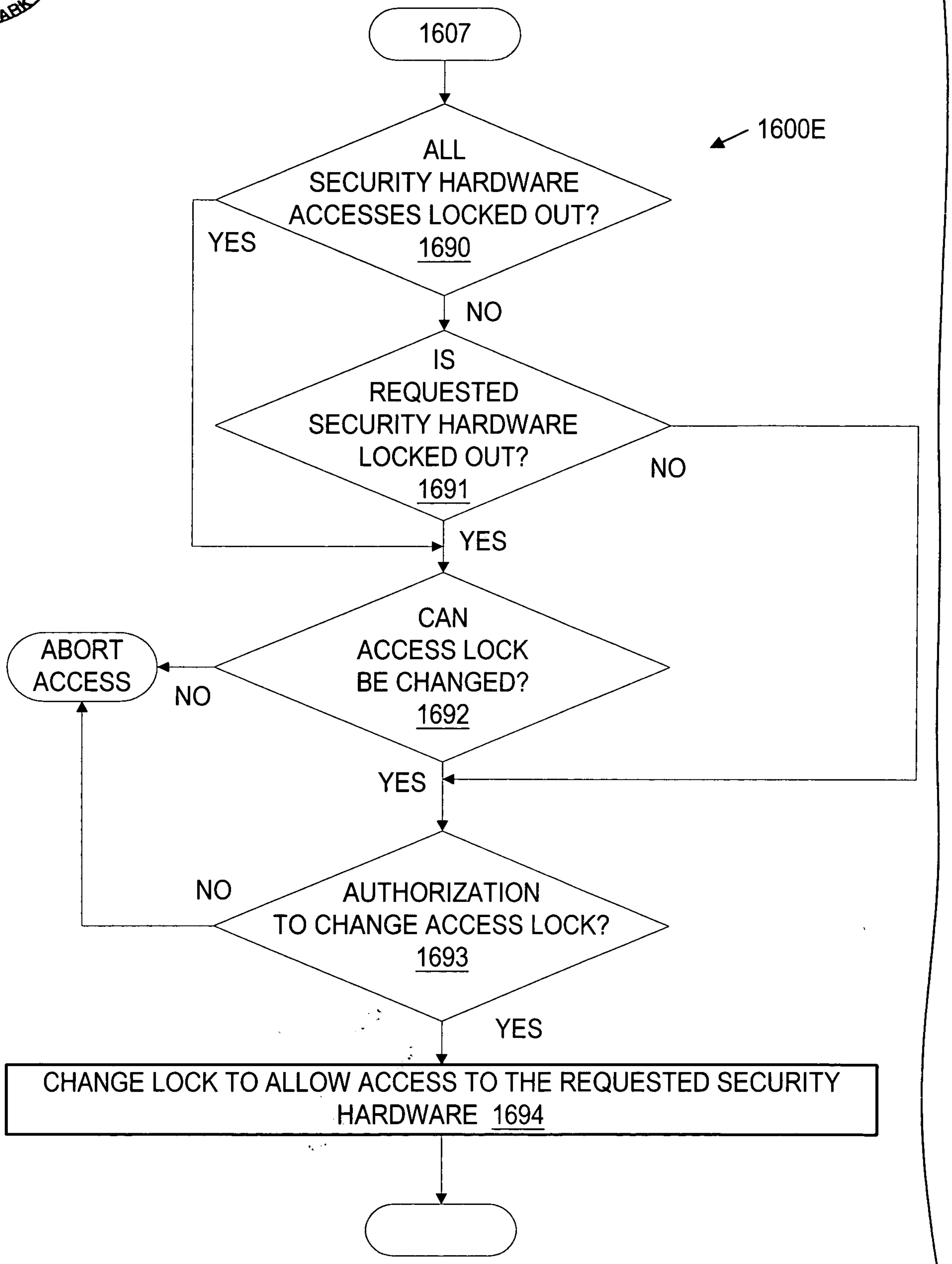

1607
1600E
ALL SECURITY HARDWARE ACCESSES LOCKED OUT? 1690
YES
NO
IS REQUESTED SECURITY HARDWARE LOCKED OUT? 1691
NO
YES
CAN ACCESS LOCK BE CHANGED? 1692
ABORT ACCESS
NO
YES
NO
AUTHORIZATION TO CHANGE ACCESS LOCK? 1693
YES
CHANGE LOCK TO ALLOW ACCESS TO THE REQUESTED SECURITY HARDWARE 1694

Fig. 16E

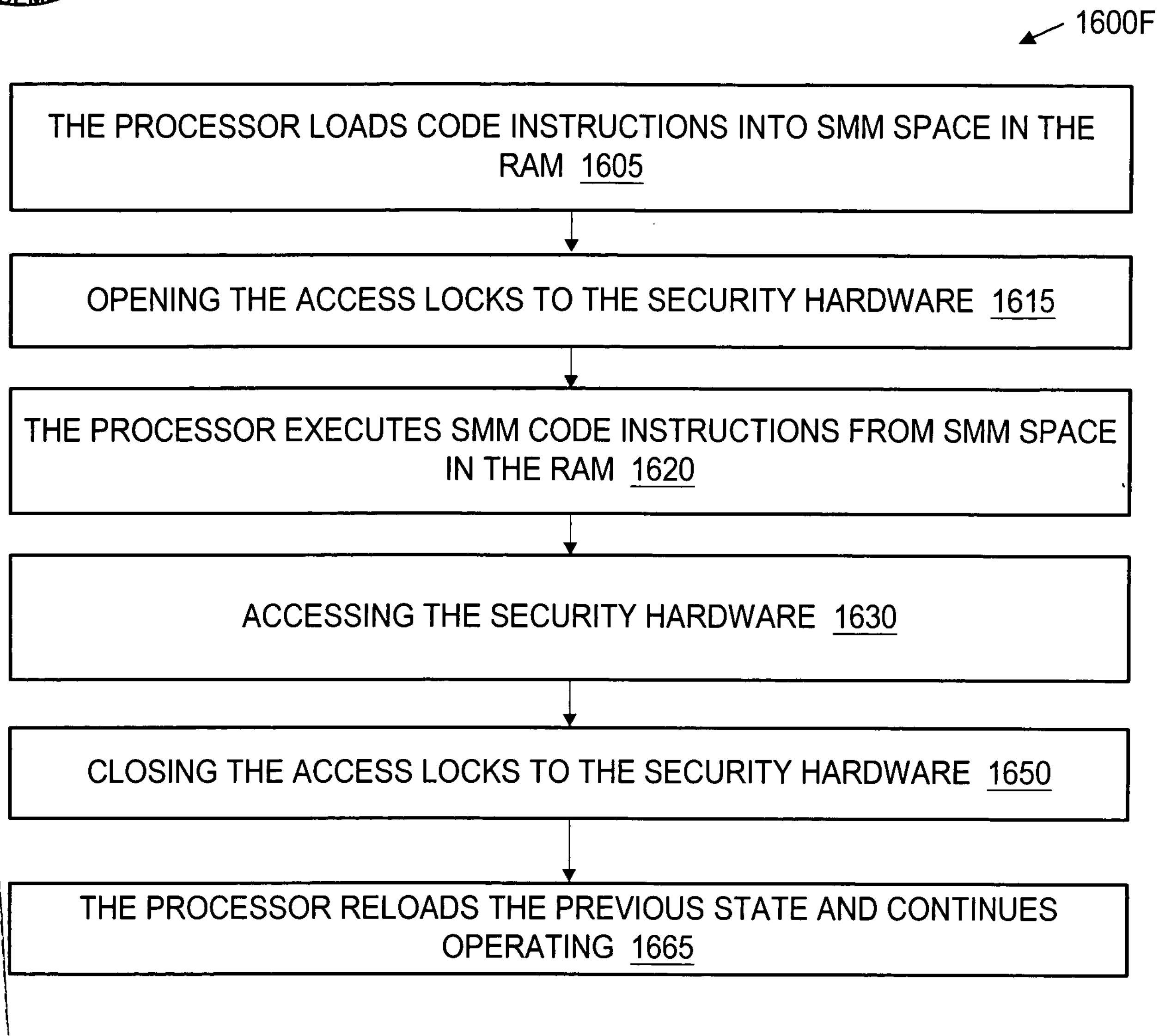

1600F
THE PROCESSOR LOADS CODE INSTRUCTIONS INTO SMM SPACE IN THE RAM 1605
OPENING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1615
THE PROCESSOR EXECUTES SMM CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620
ACCESSING THE SECURITY HARDWARE 1630
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650
THE PROCESSOR RELOADS THE PREVIOUS STATE AND CONTINUES OPERATING 1665

Fig. 16F

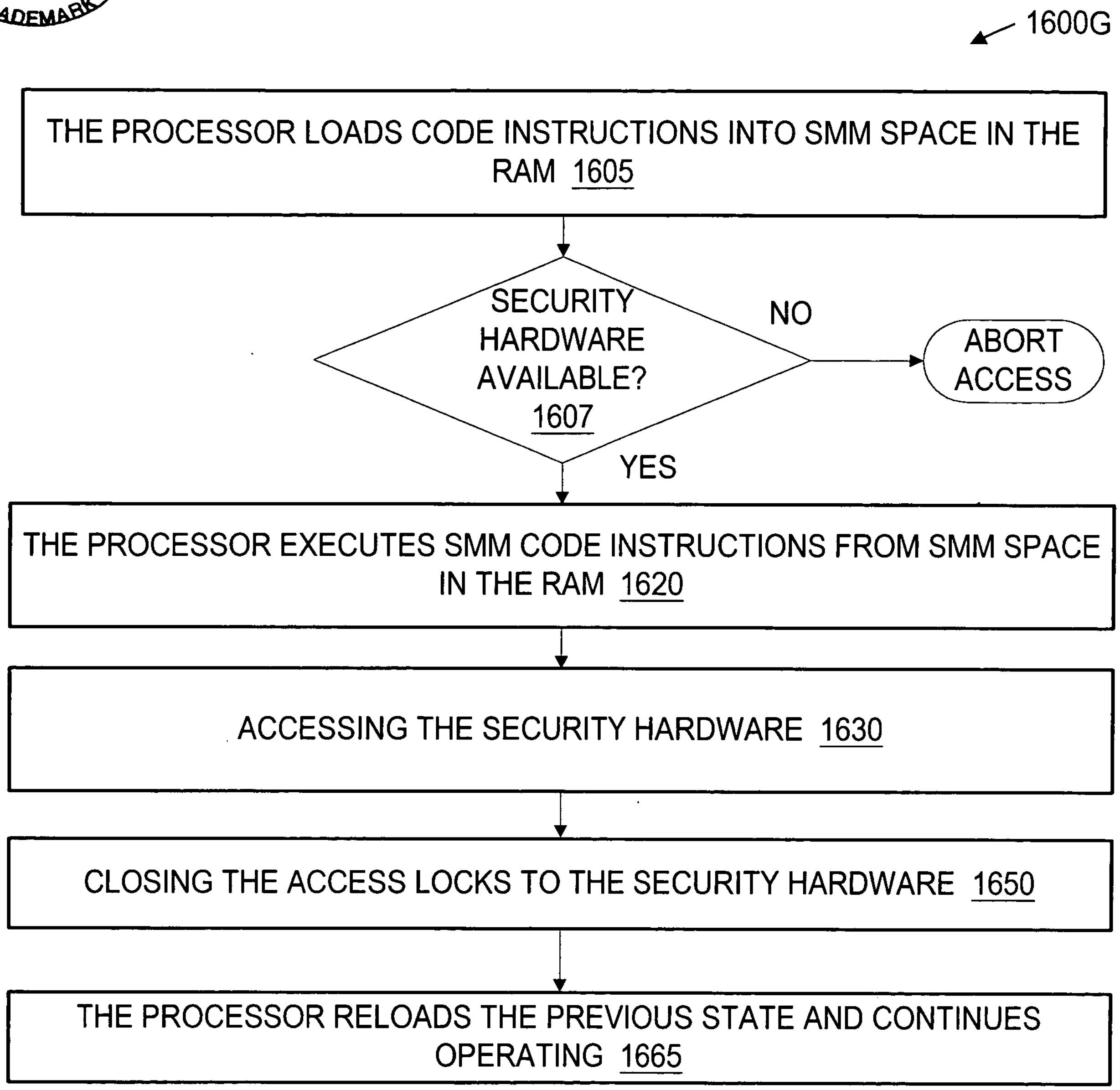

1600G
THE PROCESSOR LOADS CODE INSTRUCTIONS INTO SMM SPACE IN THE RAM 1605
SECURITY HARDWARE AVAILABLE? 1607
NO
ABORT ACCESS
YES
THE PROCESSOR EXECUTES SMM CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620
ACCESSING THE SECURITY HARDWARE 1630
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650
THE PROCESSOR RELOADS THE PREVIOUS STATE AND CONTINUES OPERATING 1665

Fig. 16G

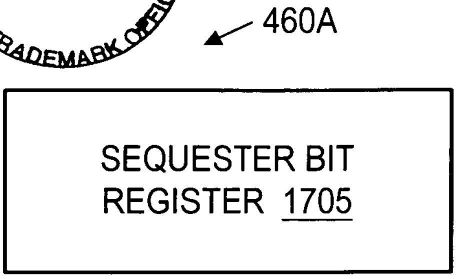


Fig. 17A

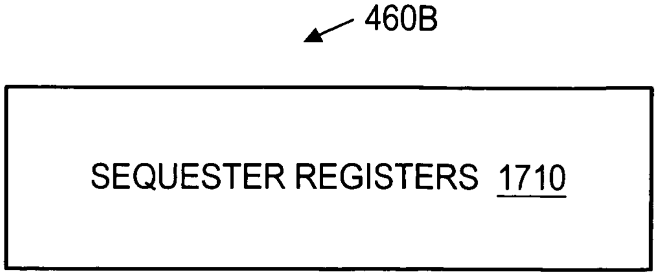


Fig. 17B

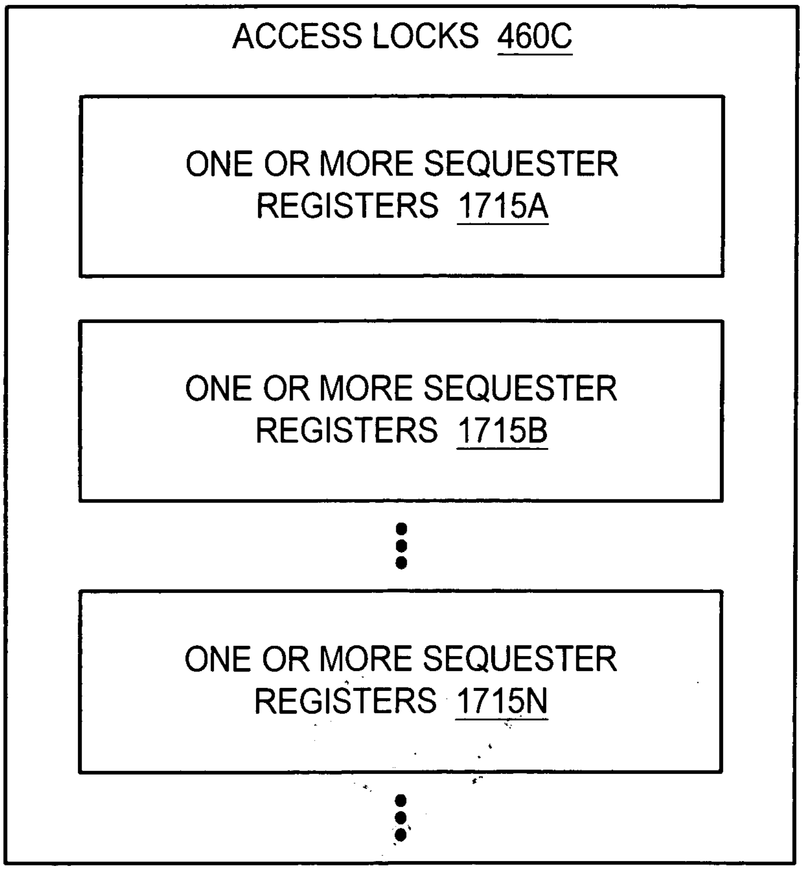

ACCESS LOCKS 460C
ONE OR MORE SEQUESTER REGISTERS 1715A
ONE OR MORE SEQUESTER REGISTERS 1715B
ONE OR MORE SEQUESTER REGISTERS 1715N

Fig. 17C

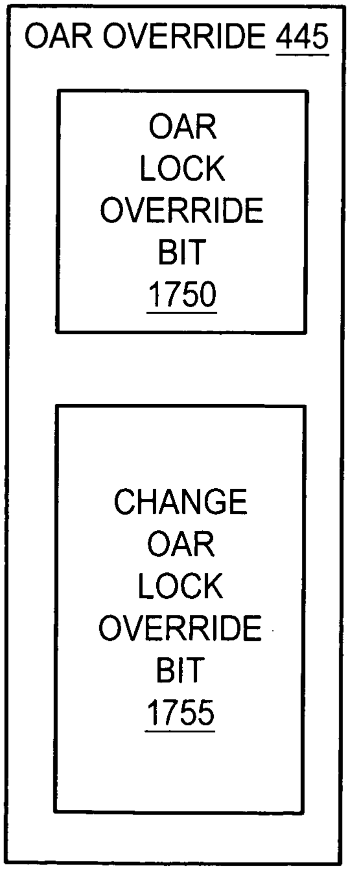


Fig. 17D

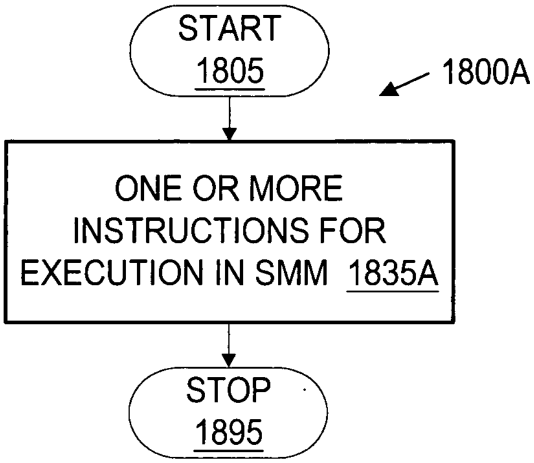


Fig. 18A
PRIOR ART

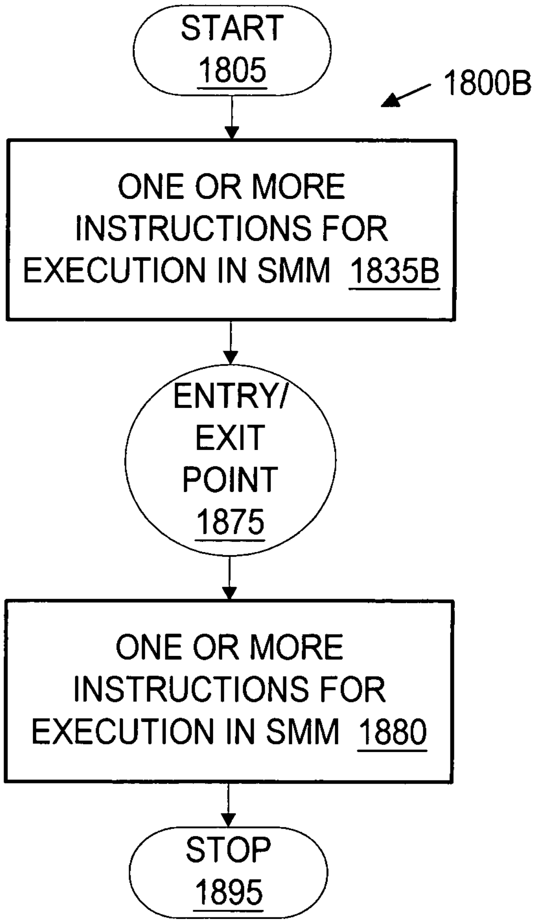

START
1805
1800B
ONE OR MORE INSTRUCTIONS FOR EXECUTION IN SMM 1835B
ENTRY/ EXIT POINT
1875
ONE OR MORE INSTRUCTIONS FOR EXECUTION IN SMM 1880
STOP
1895

Fig. 18B

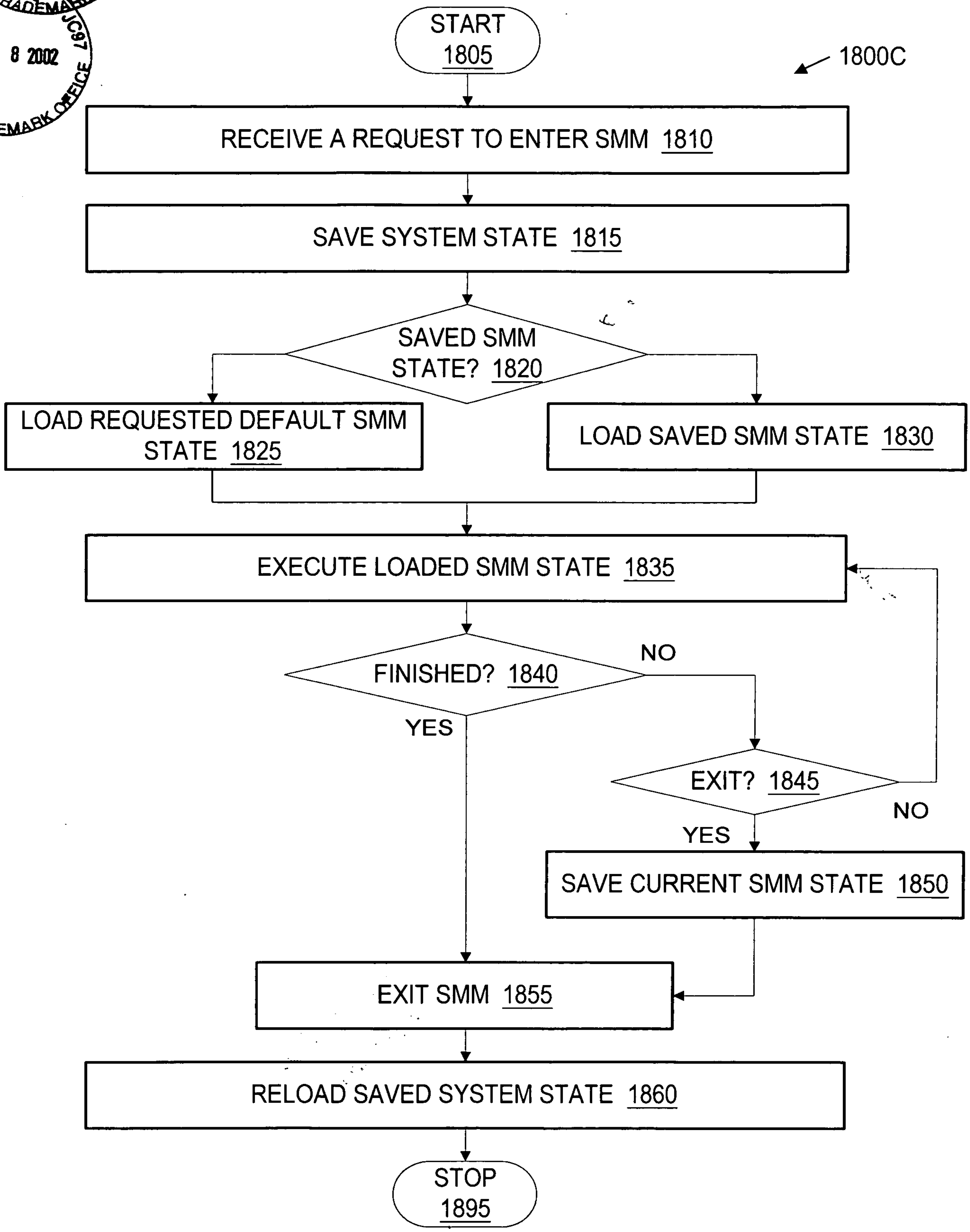

1800C
START 1805
RECEIVE A REQUEST TO ENTER SMM 1810
SAVE SYSTEM STATE 1815
SAVED SMM STATE? 1820
LOAD REQUESTED DEFAULT SMM STATE 1825
LOAD SAVED SMM STATE 1830
EXECUTE LOADED SMM STATE 1835
FINISHED? 1840
NO
YES
EXIT? 1845
NO
YES
SAVE CURRENT SMM STATE 1850
EXIT SMM 1855
RELOAD SAVED SYSTEM STATE 1860
STOP 1895

Fig. 18C

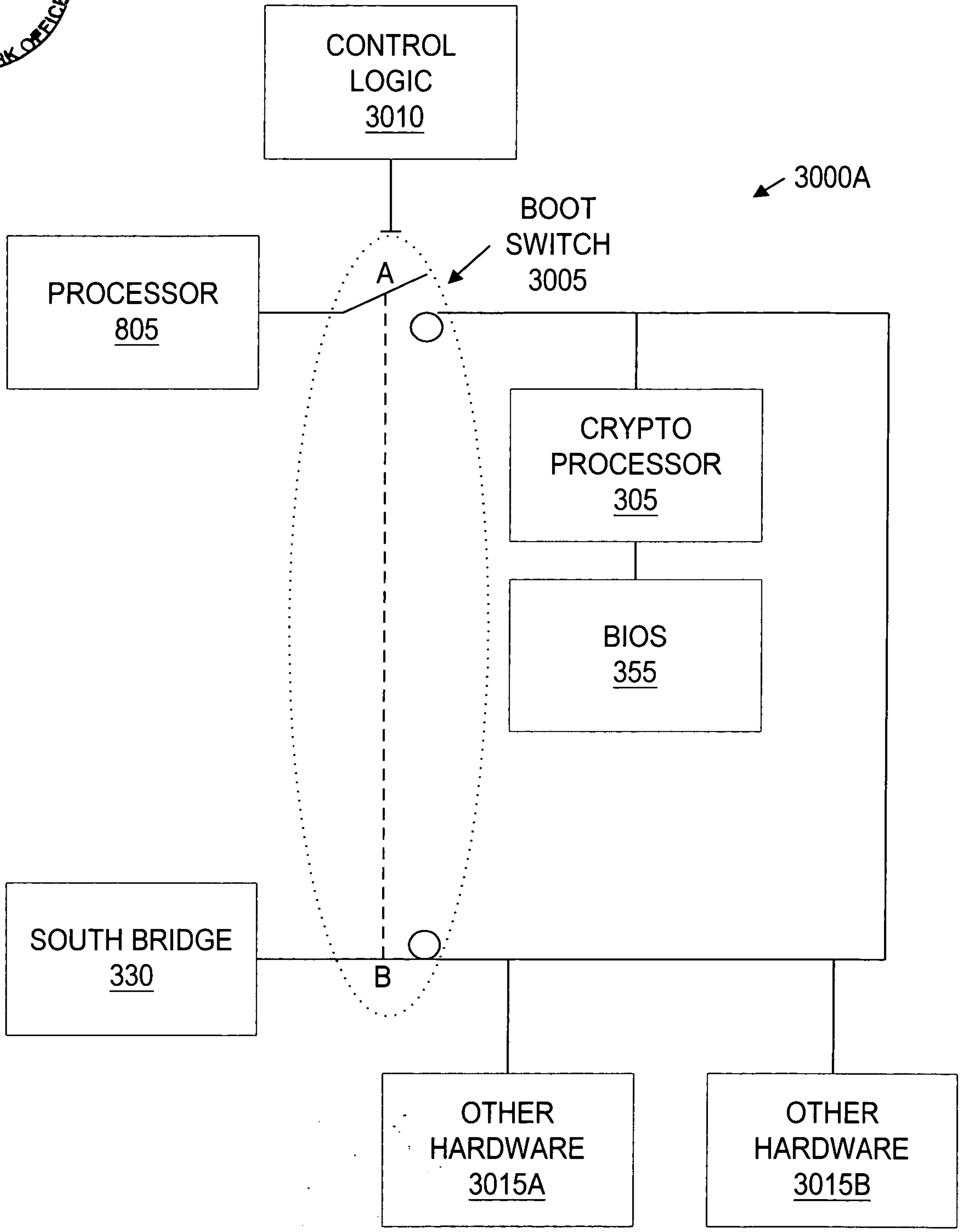

CONTROL LOGIC 3010
3000A
BOOT SWITCH 3005
PROCESSOR 805
A
CRYPTO PROCESSOR 305
BIOS 355
SOUTH BRIDGE 330
B
OTHER HARDWARE 3015A
OTHER HARDWARE 3015B

Fig. 19A

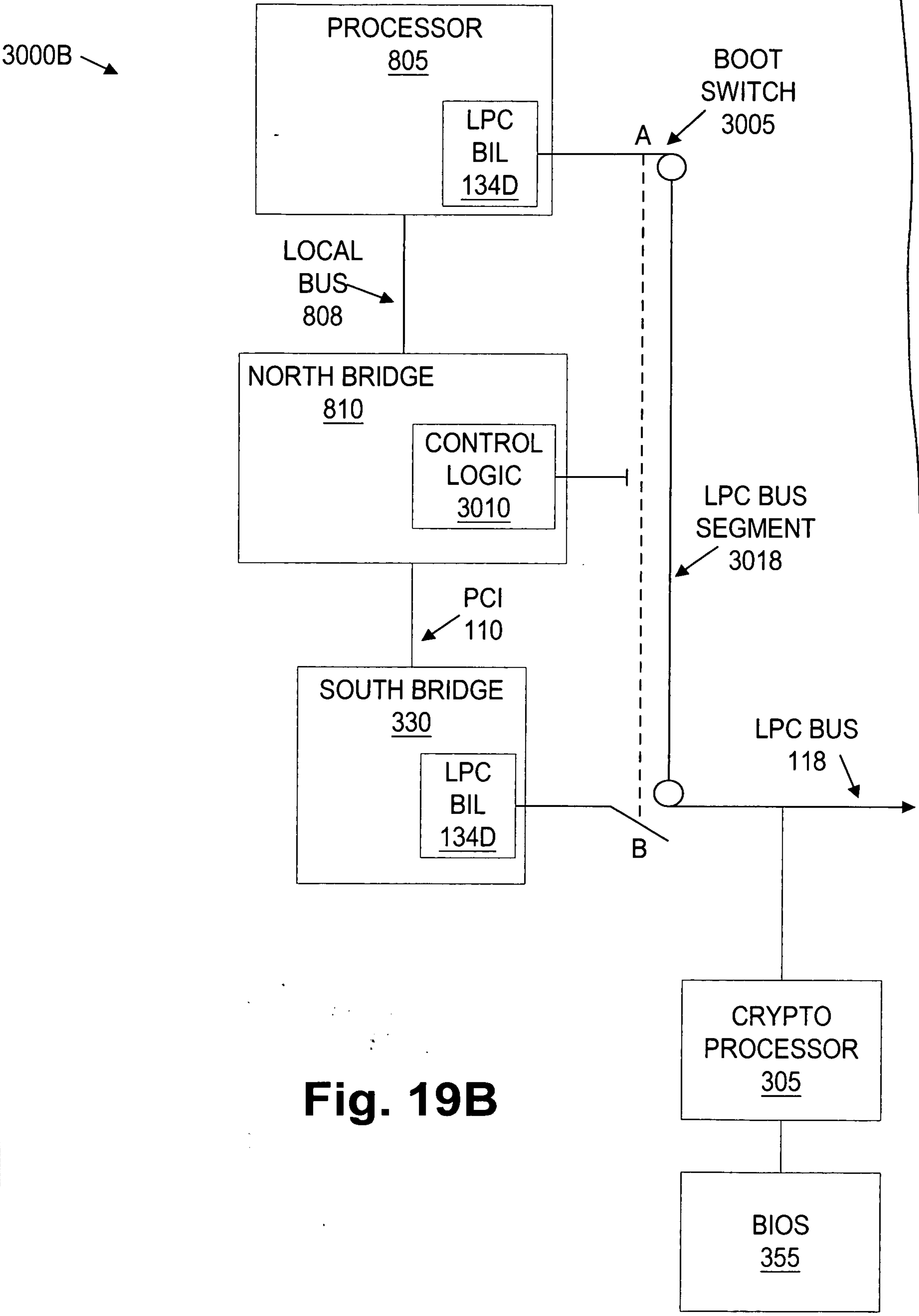

3000B
PROCESSOR
805
LPC
BIL
134D
BOOT
SWITCH
3005
A
LOCAL
BUS
808
NORTH BRIDGE
810
CONTROL
LOGIC
3010
LPC BUS
SEGMENT
3018
PCI
110
SOUTH BRIDGE
330
LPC
BIL
134D
B
LPC BUS
118
CRYPTO
PROCESSOR
305
BIOS
355

Fig. 19B

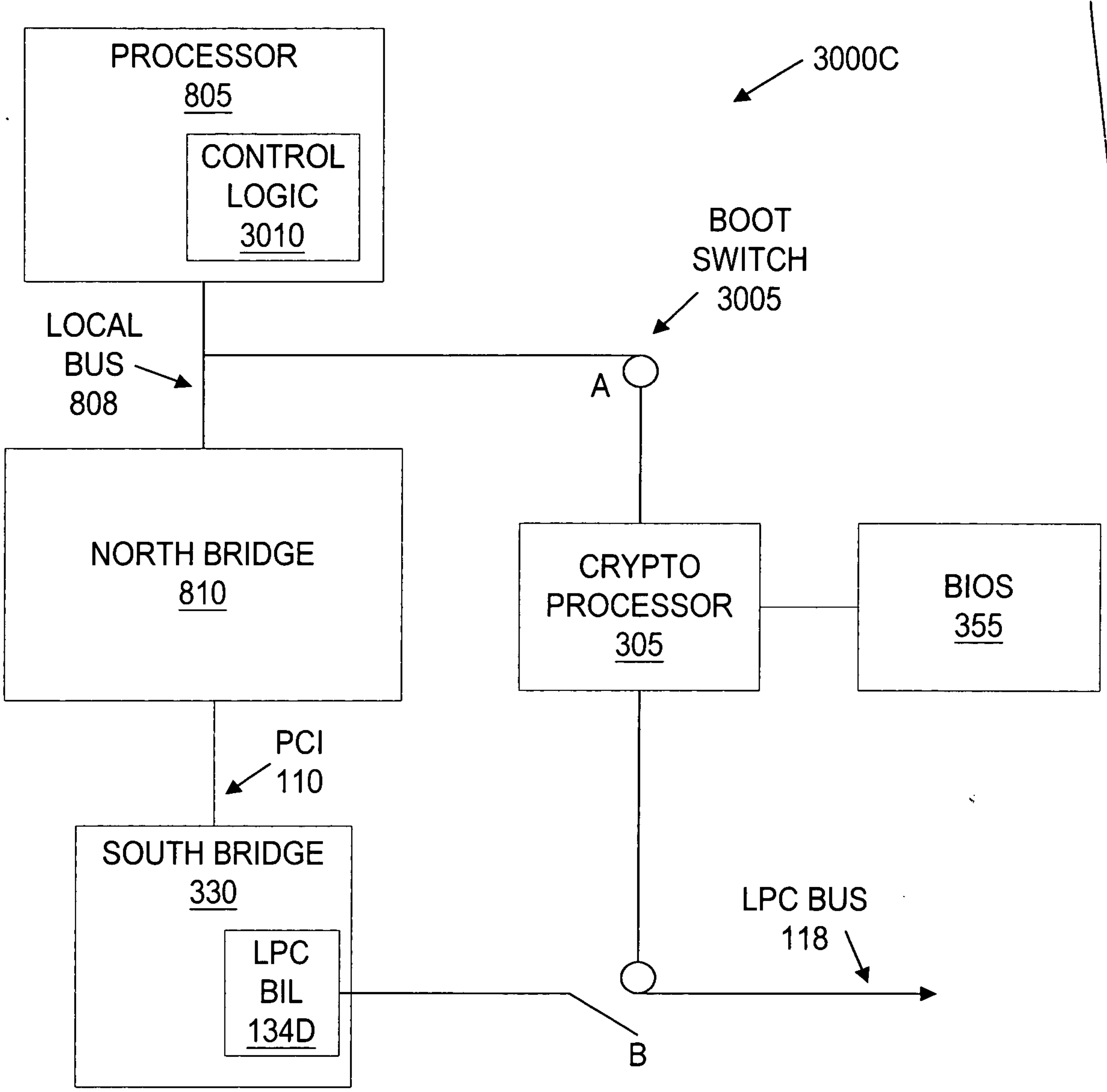

3000C
PROCESSOR
805
CONTROL
LOGIC
3010
BOOT
SWITCH
3005
LOCAL
BUS
808
A
NORTH BRIDGE
810
CRYPTO
PROCESSOR
305
BIOS
355
PCI
110
SOUTH BRIDGE
330
LPC
BIL
134D
LPC BUS
118
B

Fig. 19C

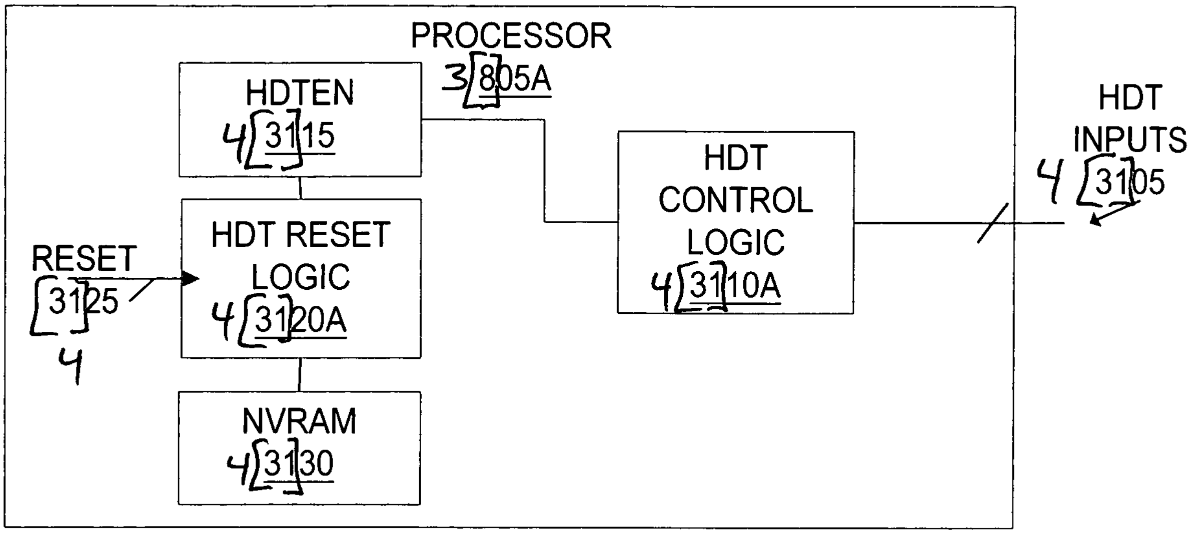


Fig. 20A
4

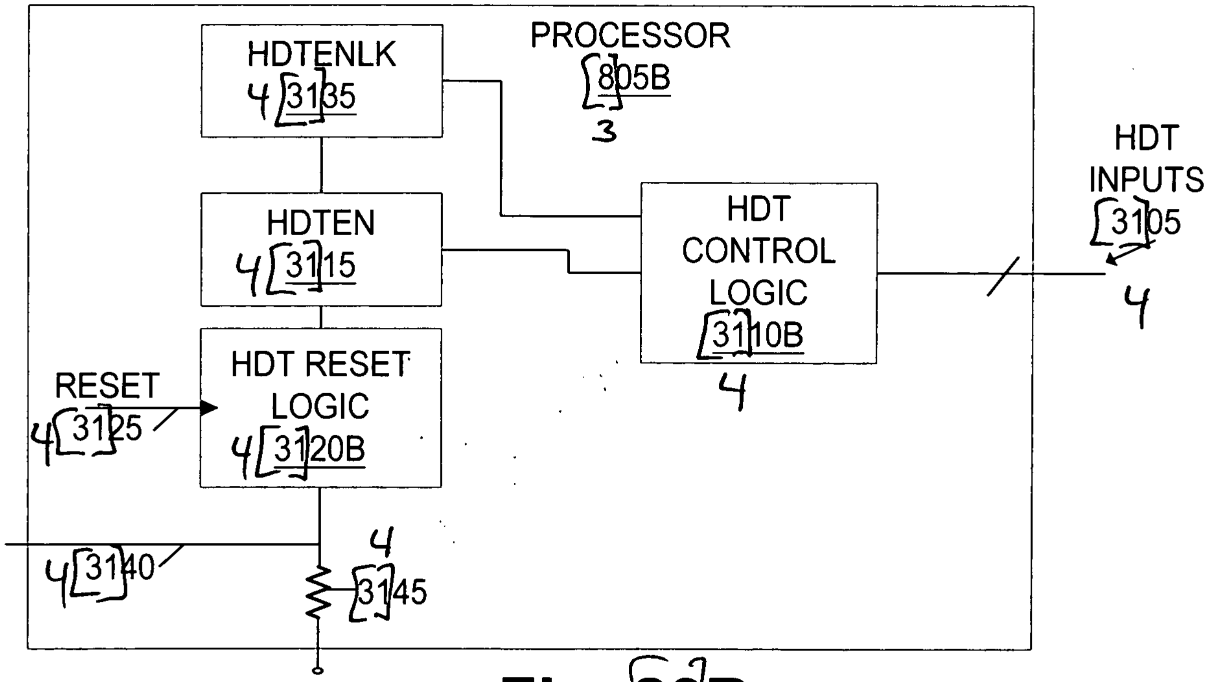


Fig. 20B
4

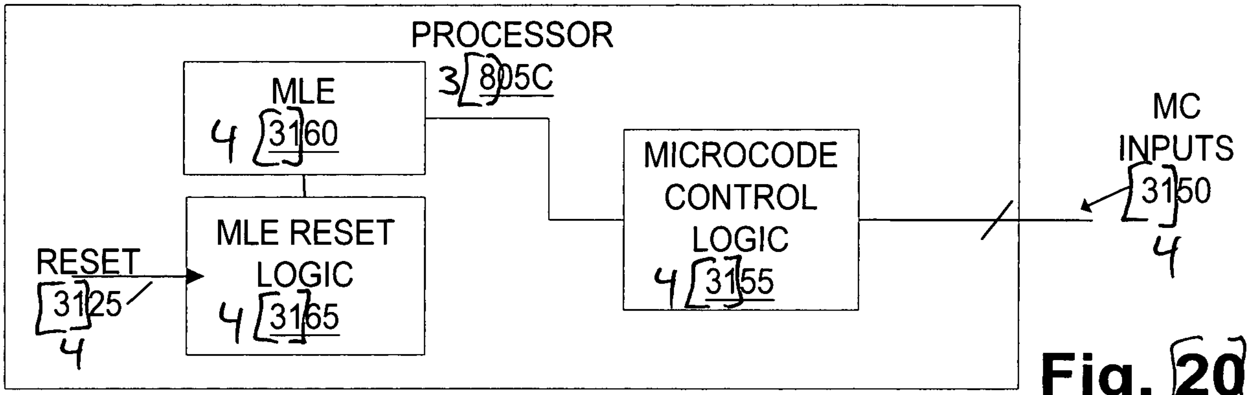


Fig. 20C
4

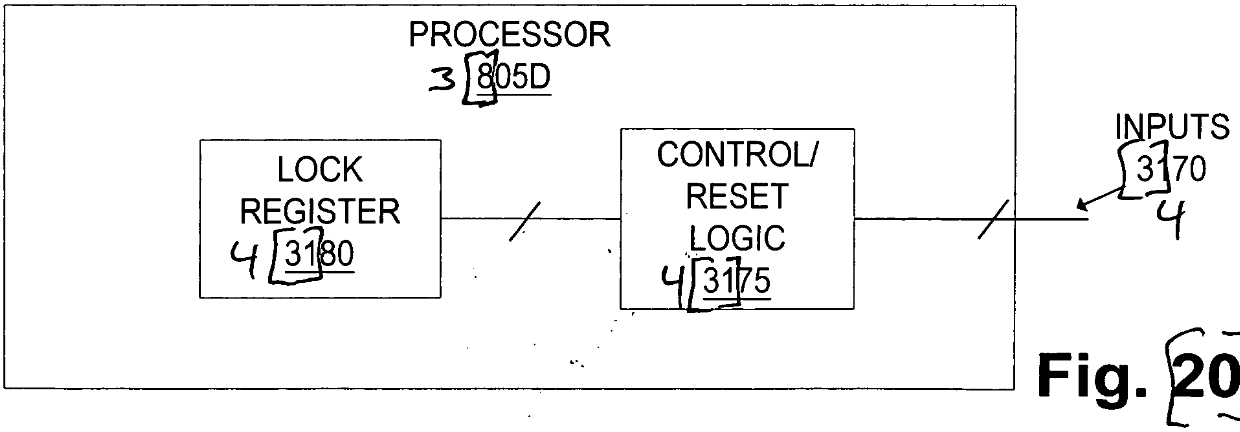


Fig. 20D
4

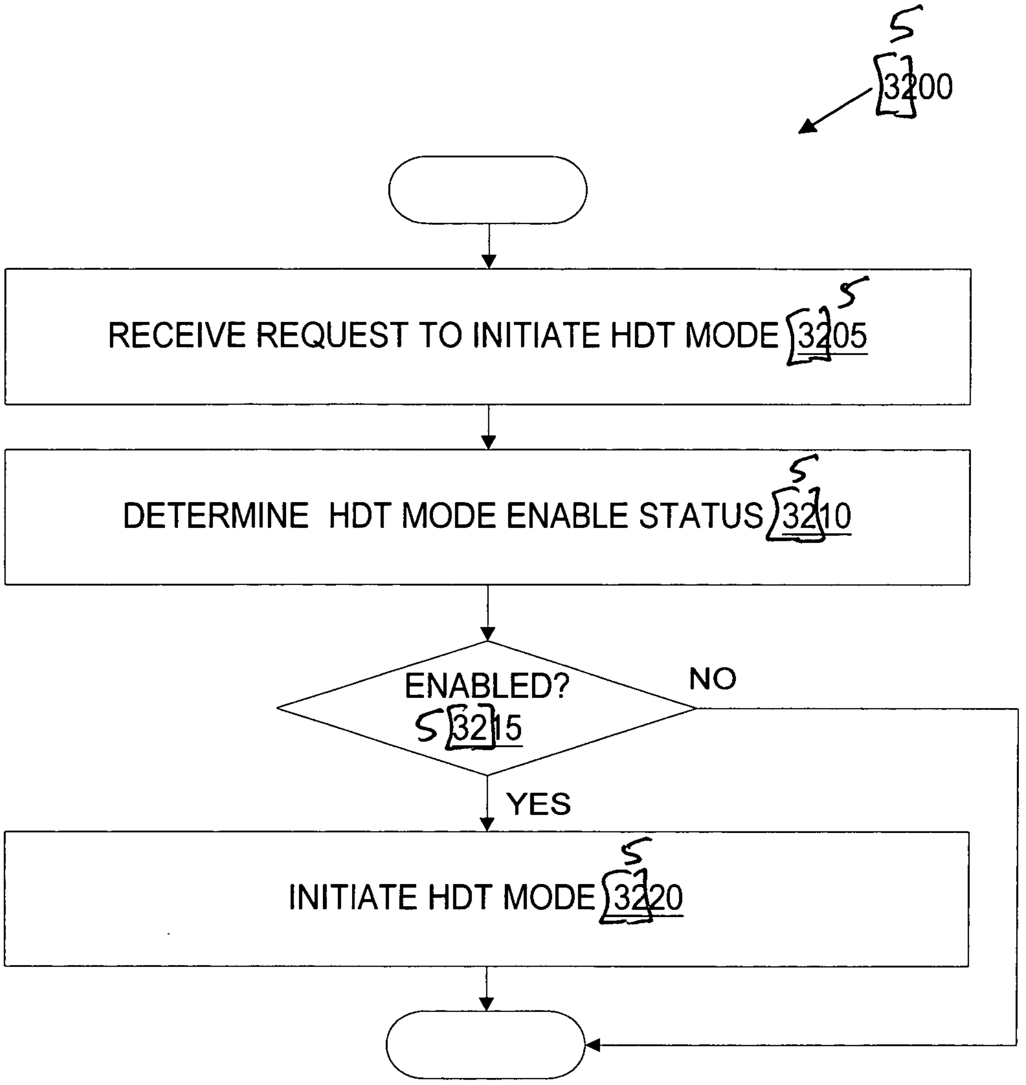

5
3200
RECEIVE REQUEST TO INITIATE HDT MODE 3205
5
DETERMINE HDT MODE ENABLE STATUS 3210
5
ENABLED?
5 3215
NO
YES
5
INITIATE HDT MODE 3220

Fig. 21 5

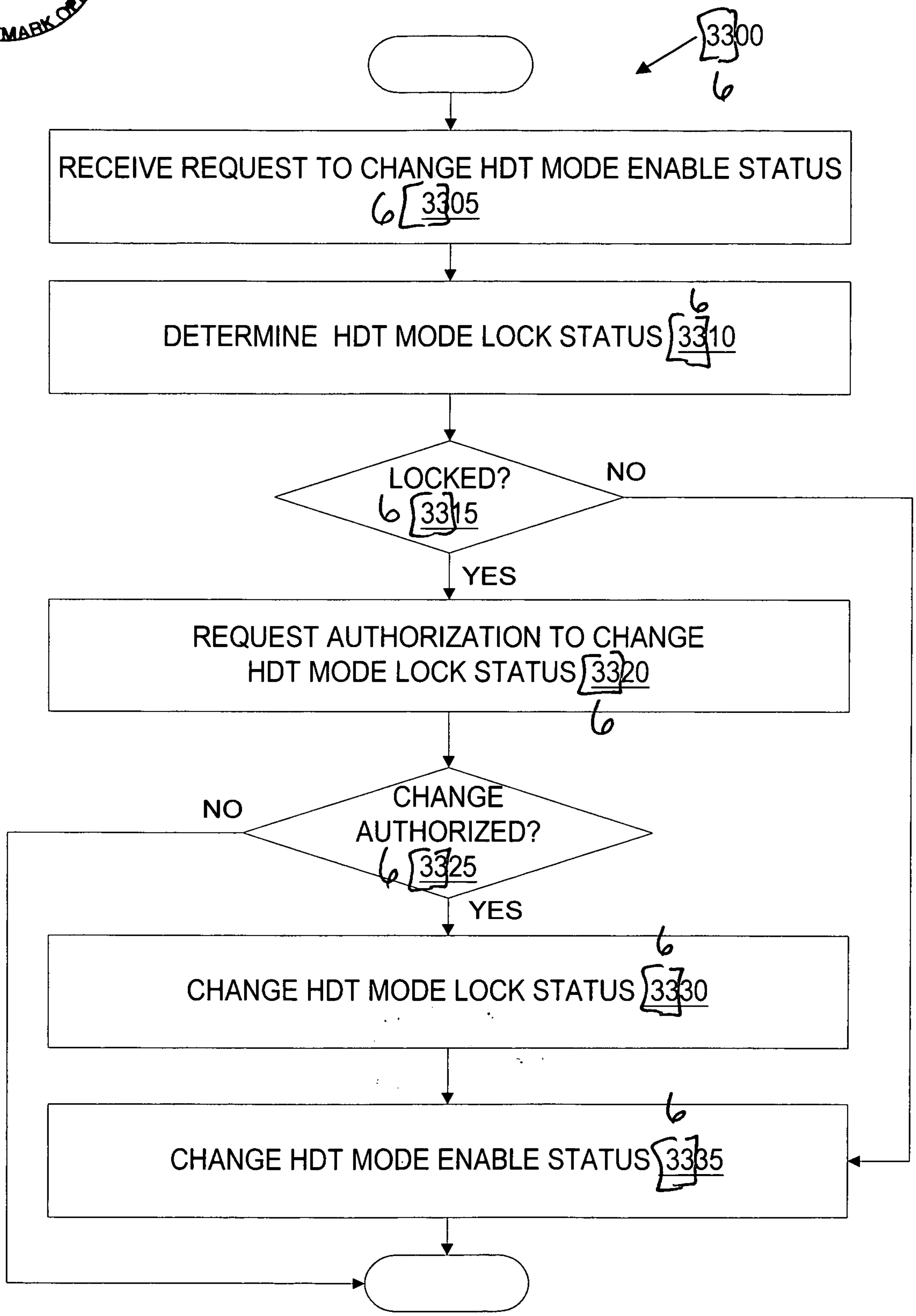

3300
6
RECEIVE REQUEST TO CHANGE HDT MODE ENABLE STATUS
6 3305
DETERMINE HDT MODE LOCK STATUS 3310
6
LOCKED?
6 3315
NO
YES
REQUEST AUTHORIZATION TO CHANGE HDT MODE LOCK STATUS 3320
6
CHANGE AUTHORIZED?
6 3325
NO
YES
CHANGE HDT MODE LOCK STATUS 3330
6
CHANGE HDT MODE ENABLE STATUS 3335
6

Fig. 22 6

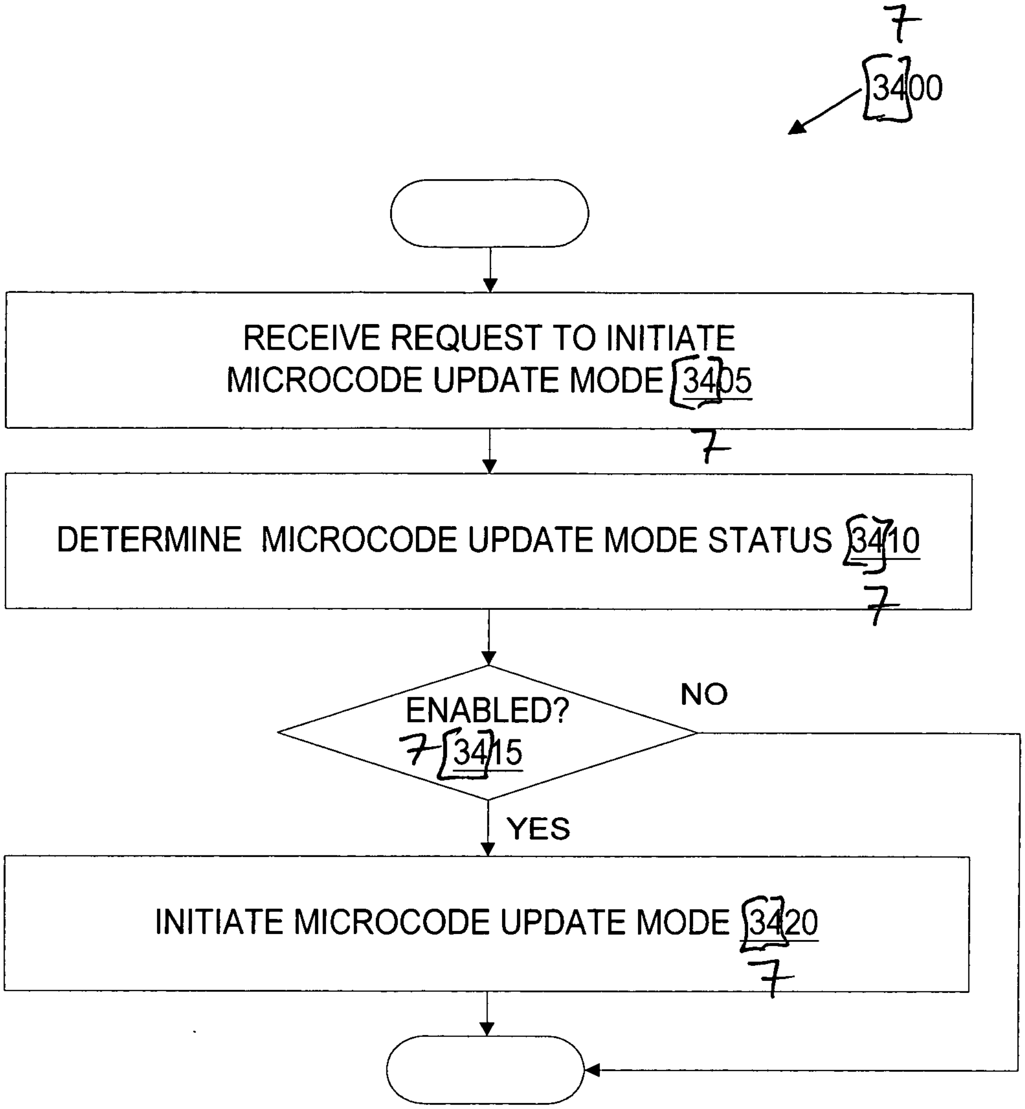

7
3400
RECEIVE REQUEST TO INITIATE MICROCODE UPDATE MODE 3405
7
DETERMINE MICROCODE UPDATE MODE STATUS 3410
7
ENABLED?
7 3415
NO
YES
INITIATE MICROCODE UPDATE MODE 3420
7

Fig. 23
7

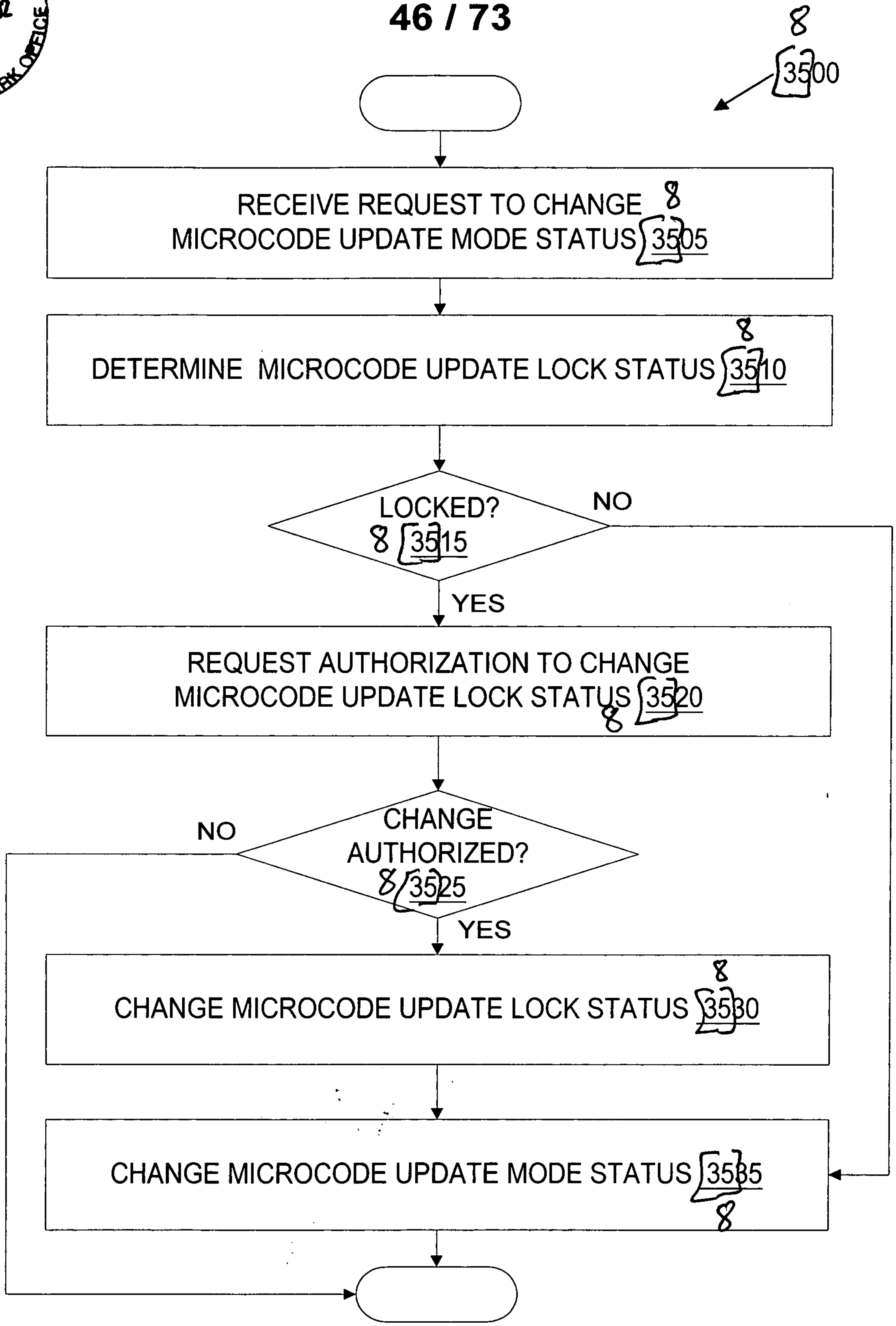

8
3500
RECEIVE REQUEST TO CHANGE MICROCODE UPDATE MODE STATUS 3505
8
DETERMINE MICROCODE UPDATE LOCK STATUS 3510
8
LOCKED?
8 3515
NO
YES
REQUEST AUTHORIZATION TO CHANGE MICROCODE UPDATE LOCK STATUS 3520
8
NO
CHANGE AUTHORIZED?
8 3525
YES
8
CHANGE MICROCODE UPDATE LOCK STATUS 3530
CHANGE MICROCODE UPDATE MODE STATUS 3535
8

Fig. 24 8

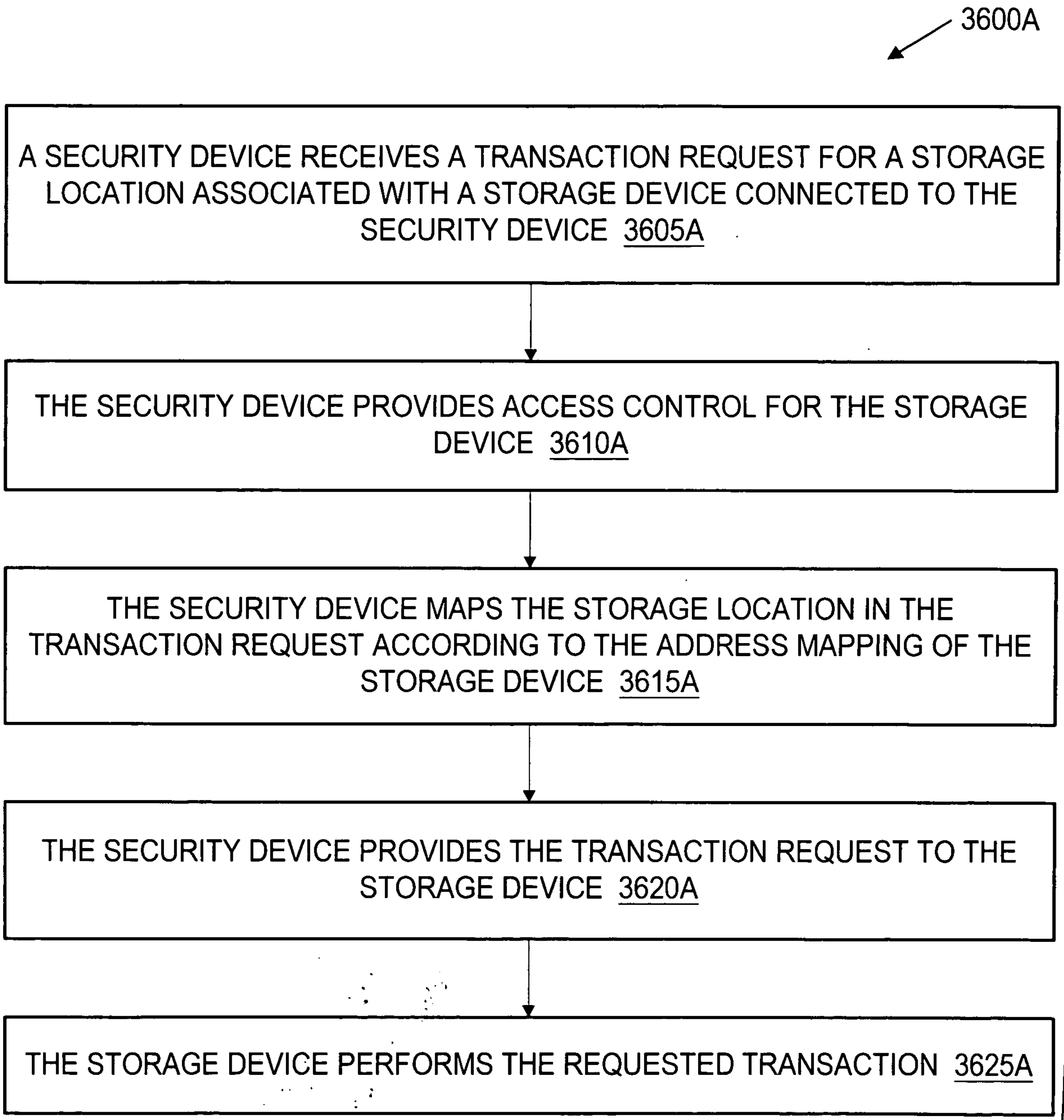

3600A
A SECURITY DEVICE RECEIVES A TRANSACTION REQUEST FOR A STORAGE LOCATION ASSOCIATED WITH A STORAGE DEVICE CONNECTED TO THE SECURITY DEVICE 3605A
THE SECURITY DEVICE PROVIDES ACCESS CONTROL FOR THE STORAGE DEVICE 3610A
THE SECURITY DEVICE MAPS THE STORAGE LOCATION IN THE TRANSACTION REQUEST ACCORDING TO THE ADDRESS MAPPING OF THE STORAGE DEVICE 3615A
THE SECURITY DEVICE PROVIDES THE TRANSACTION REQUEST TO THE STORAGE DEVICE 3620A
THE STORAGE DEVICE PERFORMS THE REQUESTED TRANSACTION 3625A

Fig. 25A

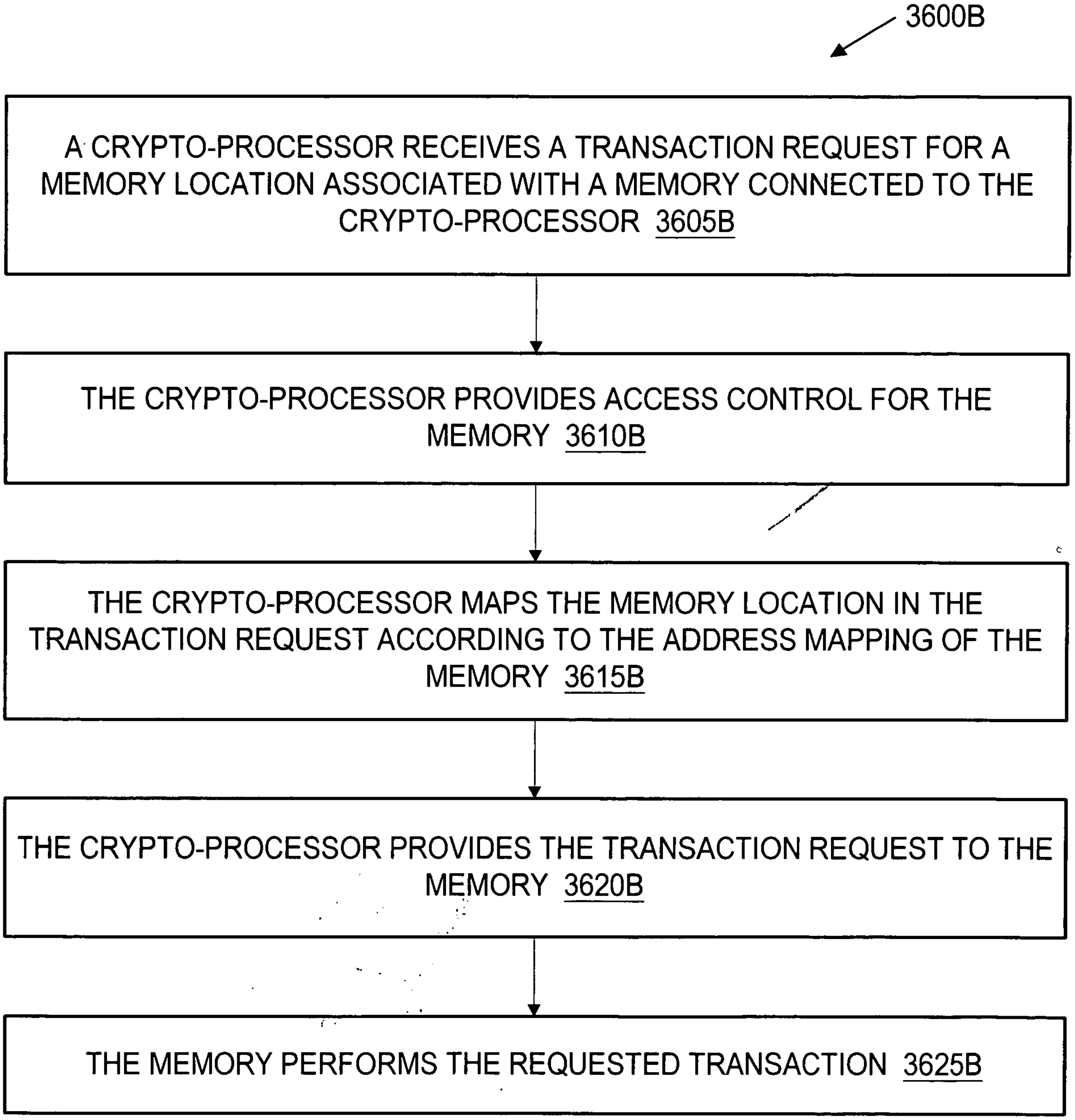

3600B
A CRYPTO-PROCESSOR RECEIVES A TRANSACTION REQUEST FOR A MEMORY LOCATION ASSOCIATED WITH A MEMORY CONNECTED TO THE CRYPTO-PROCESSOR 3605B
THE CRYPTO-PROCESSOR PROVIDES ACCESS CONTROL FOR THE MEMORY 3610B
THE CRYPTO-PROCESSOR MAPS THE MEMORY LOCATION IN THE TRANSACTION REQUEST ACCORDING TO THE ADDRESS MAPPING OF THE MEMORY 3615B
THE CRYPTO-PROCESSOR PROVIDES THE TRANSACTION REQUEST TO THE MEMORY 3620B
THE MEMORY PERFORMS THE REQUESTED TRANSACTION 3625B

Fig. 25B

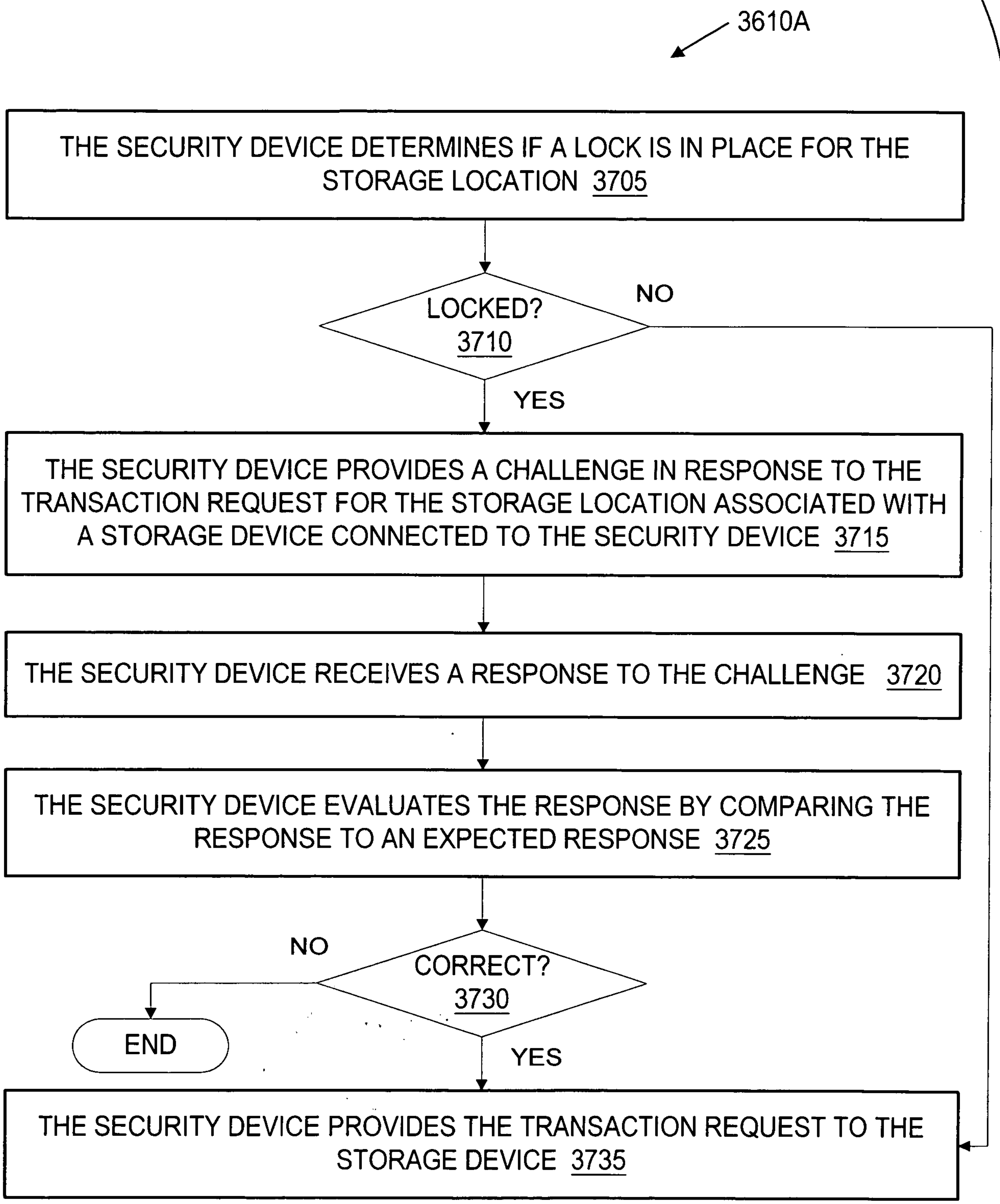

3610A
THE SECURITY DEVICE DETERMINES IF A LOCK IS IN PLACE FOR THE STORAGE LOCATION 3705
LOCKED? 3710
NO
YES
THE SECURITY DEVICE PROVIDES A CHALLENGE IN RESPONSE TO THE TRANSACTION REQUEST FOR THE STORAGE LOCATION ASSOCIATED WITH A STORAGE DEVICE CONNECTED TO THE SECURITY DEVICE 3715
THE SECURITY DEVICE RECEIVES A RESPONSE TO THE CHALLENGE 3720
THE SECURITY DEVICE EVALUATES THE RESPONSE BY COMPARING THE RESPONSE TO AN EXPECTED RESPONSE 3725
NO
CORRECT? 3730
END
YES
THE SECURITY DEVICE PROVIDES THE TRANSACTION REQUEST TO THE STORAGE DEVICE 3735

Fig. 26

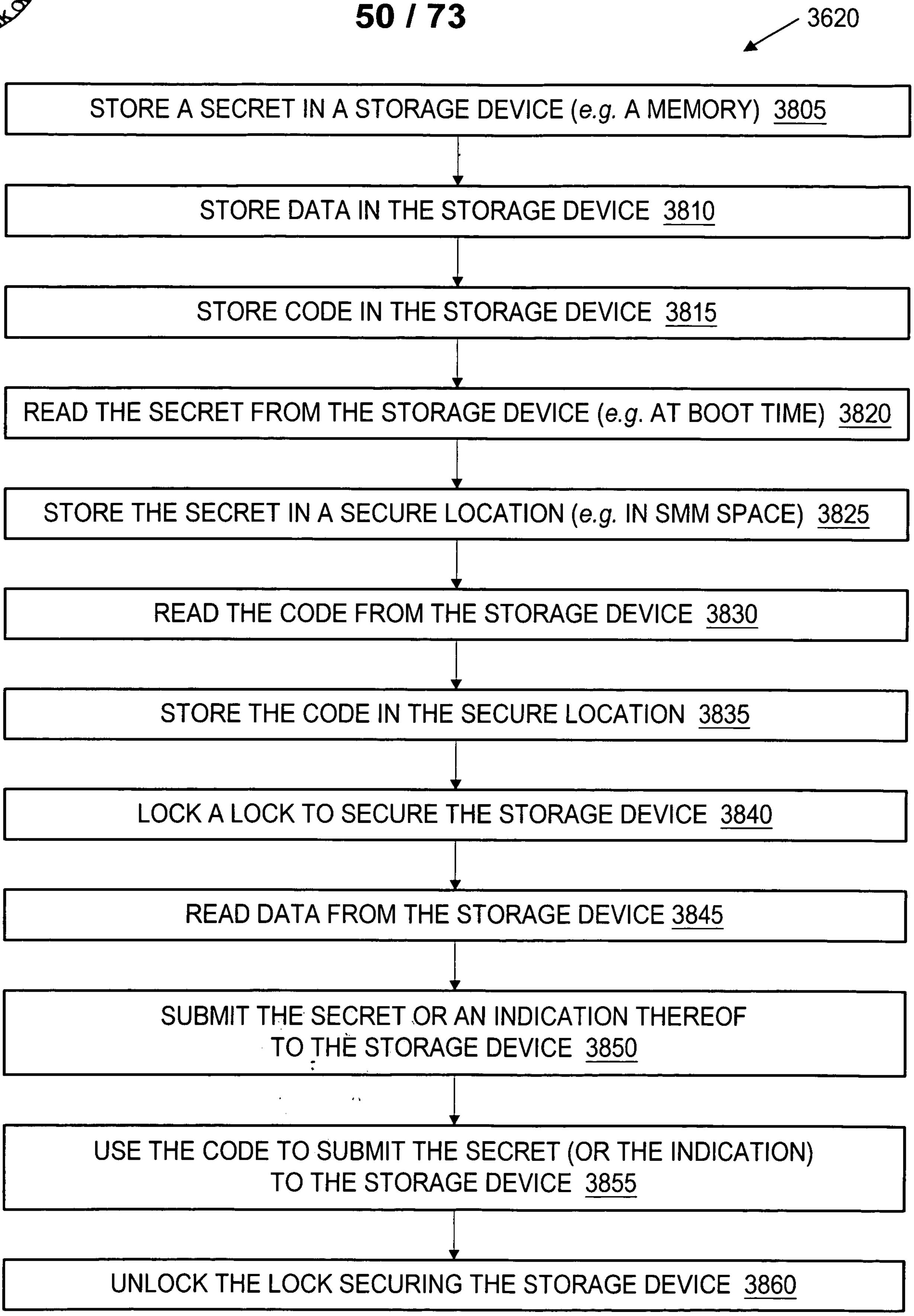

3620
STORE A SECRET IN A STORAGE DEVICE (e.g. A MEMORY) 3805
STORE DATA IN THE STORAGE DEVICE 3810
STORE CODE IN THE STORAGE DEVICE 3815
READ THE SECRET FROM THE STORAGE DEVICE (e.g. AT BOOT TIME) 3820
STORE THE SECRET IN A SECURE LOCATION (e.g. IN SMM SPACE) 3825
READ THE CODE FROM THE STORAGE DEVICE 3830
STORE THE CODE IN THE SECURE LOCATION 3835
LOCK A LOCK TO SECURE THE STORAGE DEVICE 3840
READ DATA FROM THE STORAGE DEVICE 3845
SUBMIT THE SECRET OR AN INDICATION THEREOF TO THE STORAGE DEVICE 3850
USE THE CODE TO SUBMIT THE SECRET (OR THE INDICATION) TO THE STORAGE DEVICE 3855
UNLOCK THE LOCK SECURING THE STORAGE DEVICE 3860

Fig. 27

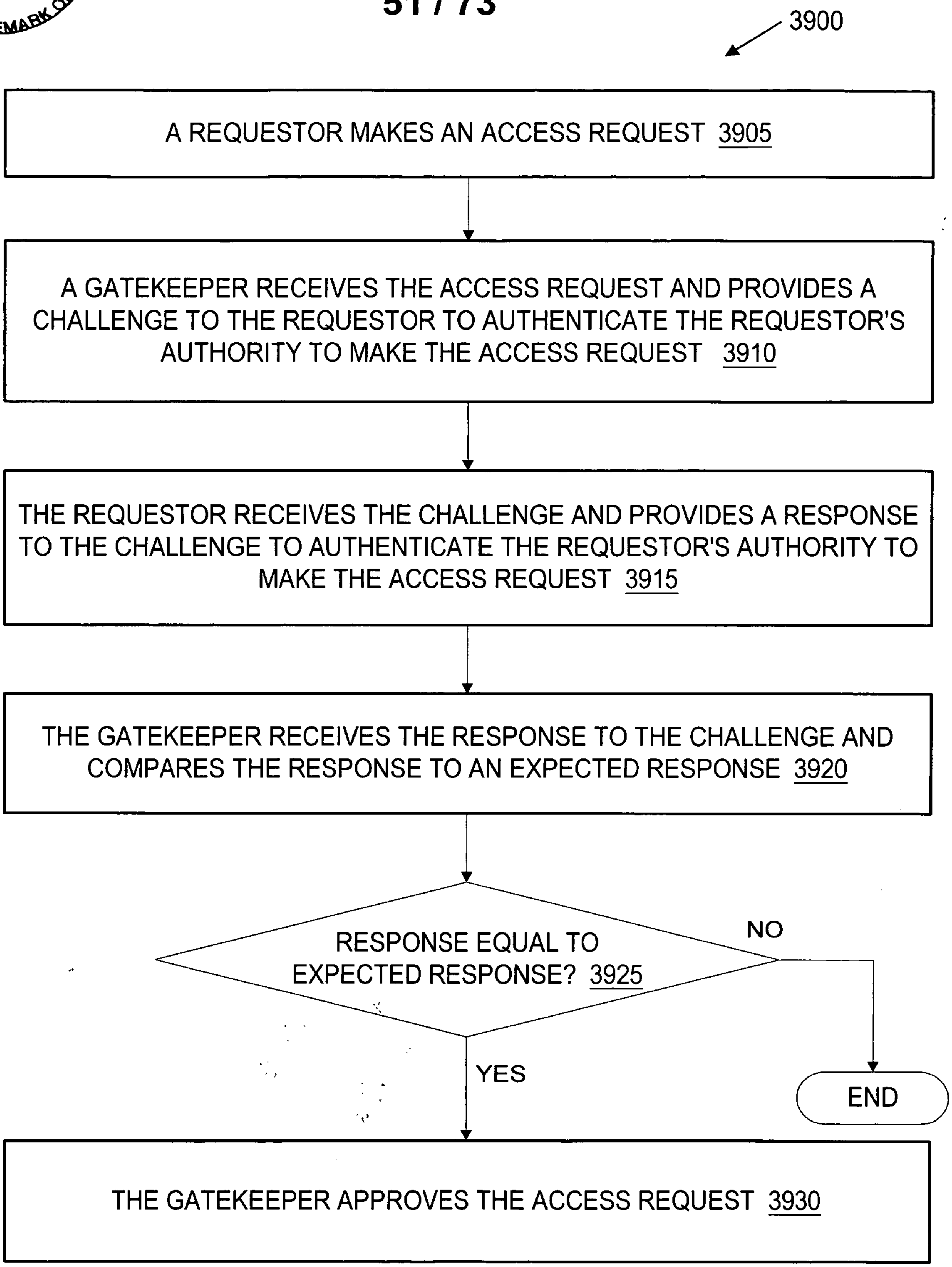

3900
A REQUESTOR MAKES AN ACCESS REQUEST 3905
A GATEKEEPER RECEIVES THE ACCESS REQUEST AND PROVIDES A CHALLENGE TO THE REQUESTOR TO AUTHENTICATE THE REQUESTOR'S AUTHORITY TO MAKE THE ACCESS REQUEST 3910
THE REQUESTOR RECEIVES THE CHALLENGE AND PROVIDES A RESPONSE TO THE CHALLENGE TO AUTHENTICATE THE REQUESTOR'S AUTHORITY TO MAKE THE ACCESS REQUEST 3915
THE GATEKEEPER RECEIVES THE RESPONSE TO THE CHALLENGE AND COMPARES THE RESPONSE TO AN EXPECTED RESPONSE 3920
RESPONSE EQUAL TO EXPECTED RESPONSE? 3925
NO
END
YES
THE GATEKEEPER APPROVES THE ACCESS REQUEST 3930

Fig. 28
(Prior Art)

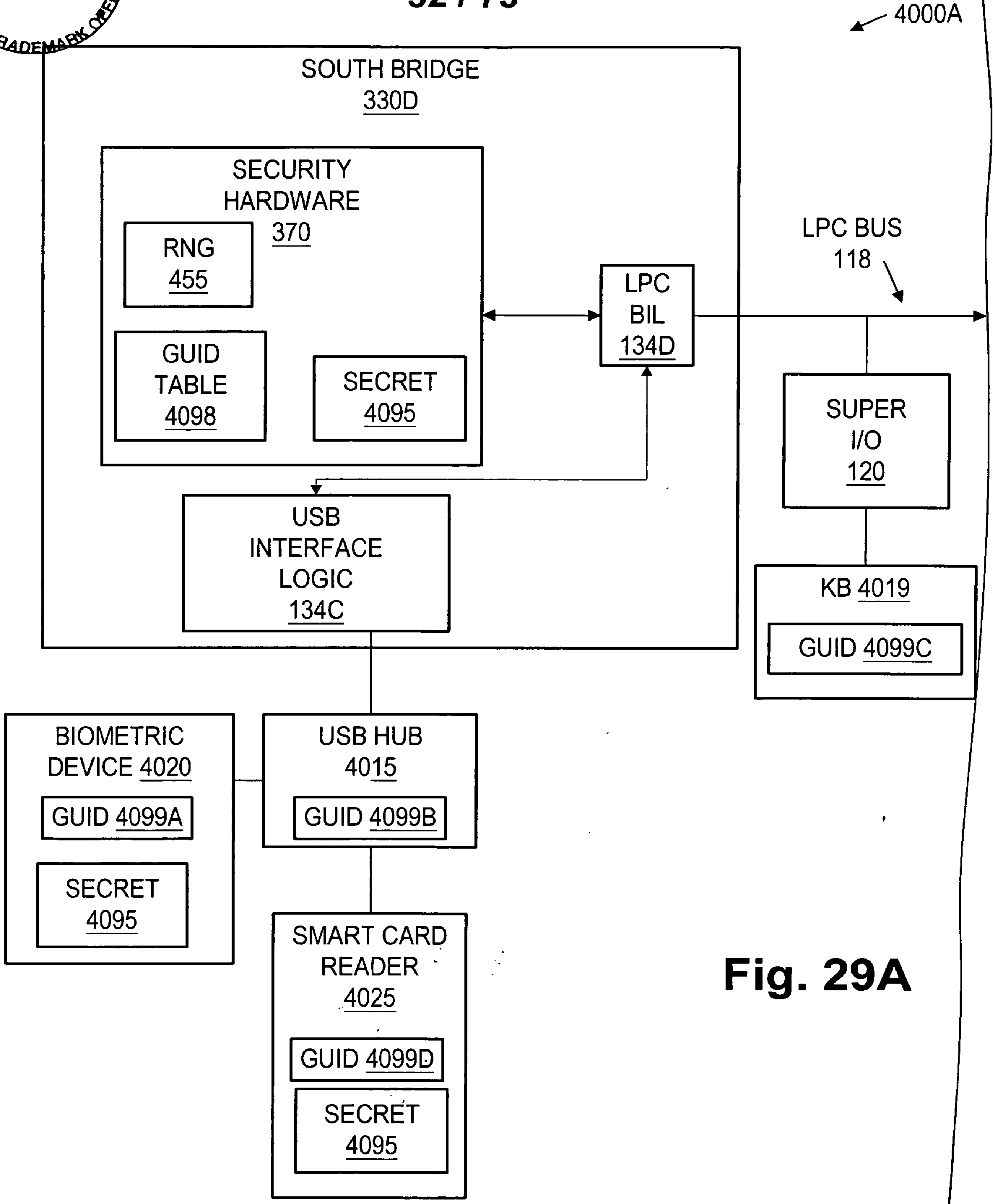

4000A
SOUTH BRIDGE 330D
SECURITY HARDWARE 370
RNG 455
GUID TABLE 4098
SECRET 4095
LPC BIL 134D
LPC BUS 118
SUPER I/O 120
KB 4019
GUID 4099C
USB INTERFACE LOGIC 134C
BIOMETRIC DEVICE 4020
GUID 4099A
SECRET 4095
USB HUB 4015
GUID 4099B
SMART CARD READER 4025
GUID 4099D
SECRET 4095

Fig. 29A

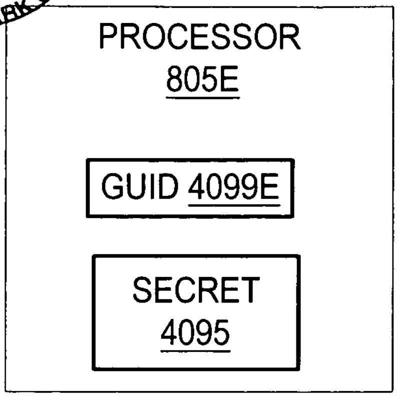


Fig. 29B

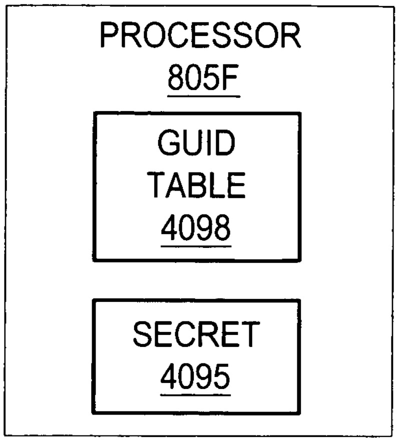


Fig. 29C

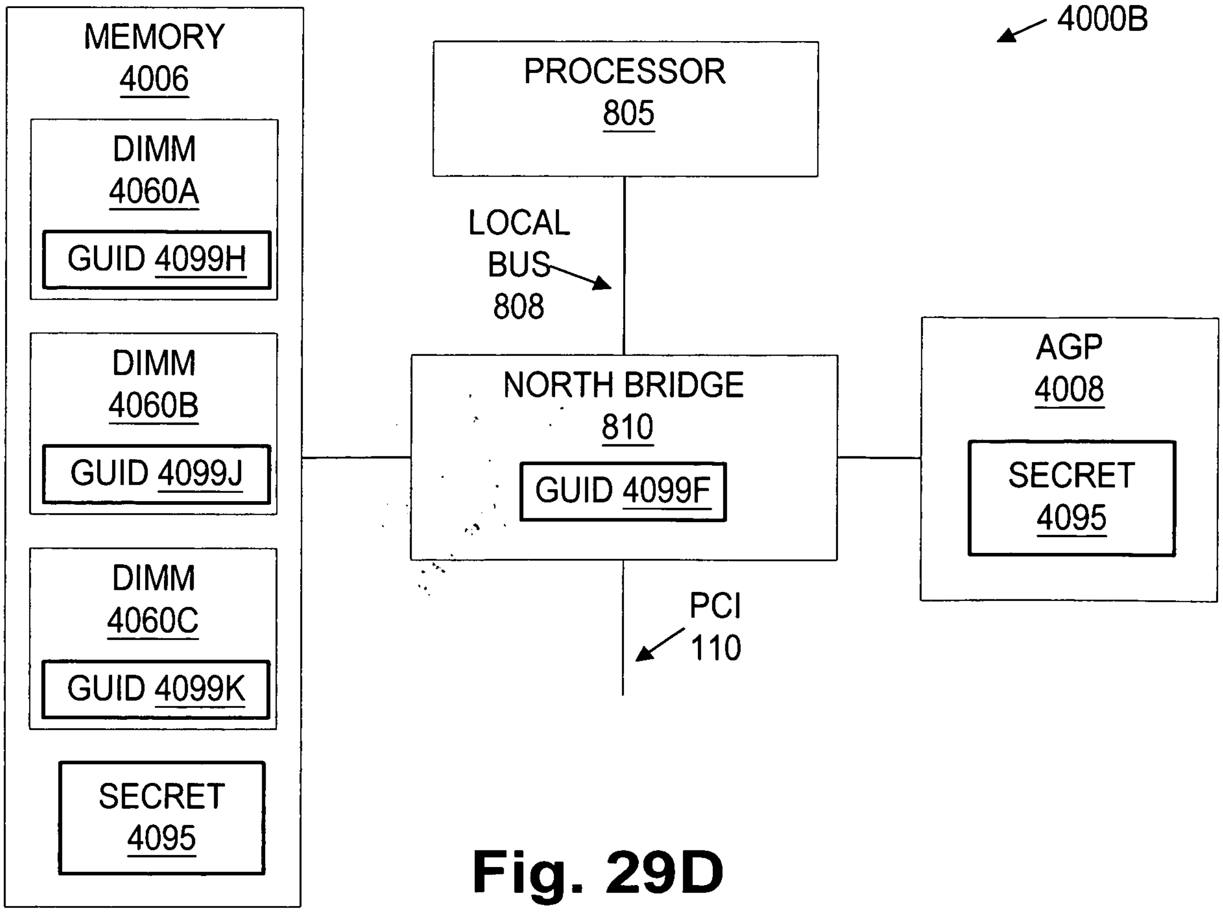


Fig. 29D

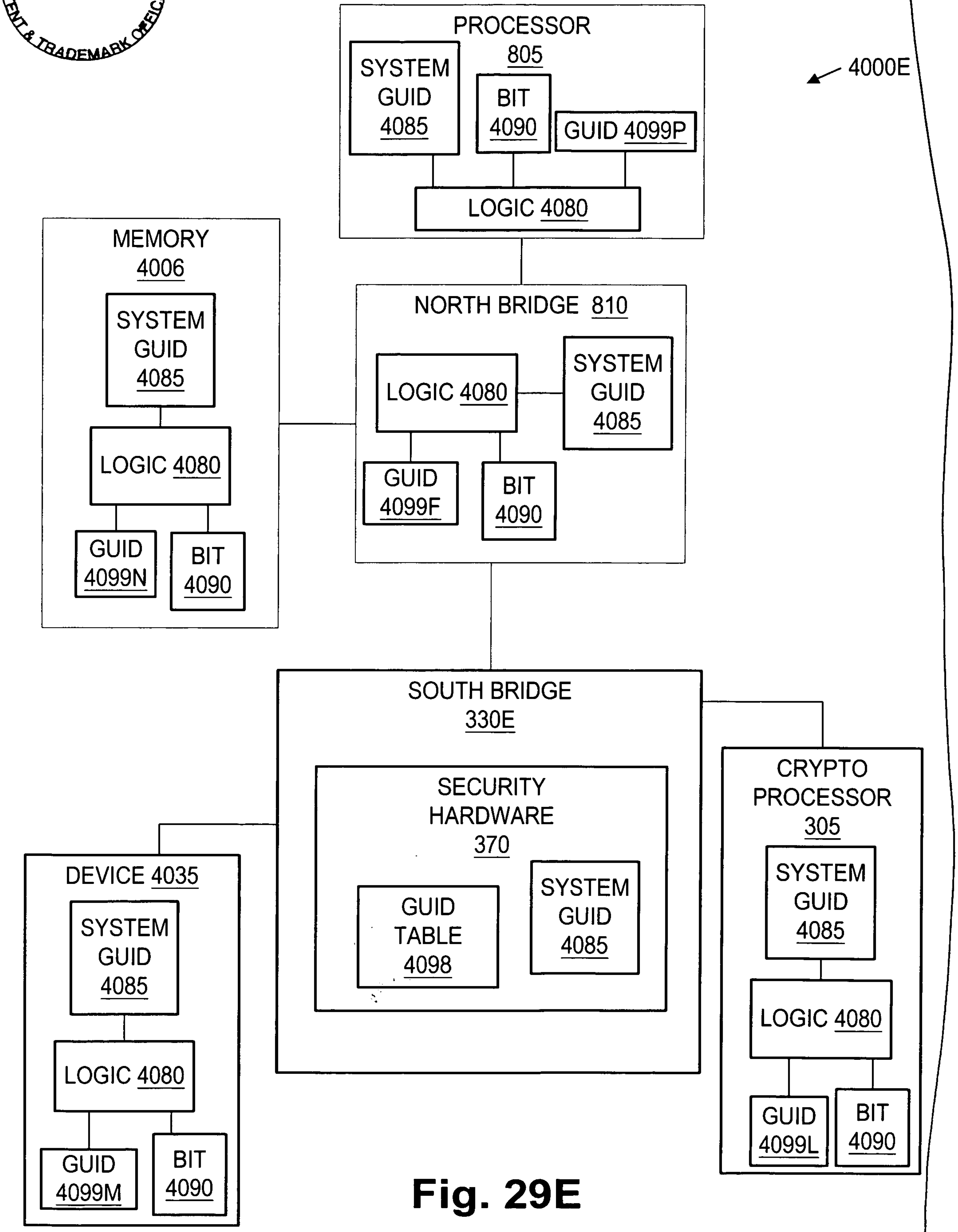

PROCESSOR 805
SYSTEM GUID 4085
BIT 4090
GUID 4099P
LOGIC 4080
4000E
MEMORY 4006
SYSTEM GUID 4085
LOGIC 4080
GUID 4099N
BIT 4090
NORTH BRIDGE 810
LOGIC 4080
SYSTEM GUID 4085
GUID 4099F
BIT 4090
SOUTH BRIDGE 330E
SECURITY HARDWARE 370
GUID TABLE 4098
SYSTEM GUID 4085
CRYPTO PROCESSOR 305
SYSTEM GUID 4085
LOGIC 4080
GUID 4099L
BIT 4090
DEVICE 4035
SYSTEM GUID 4085
LOGIC 4080
GUID 4099M
BIT 4090

Fig. 29E

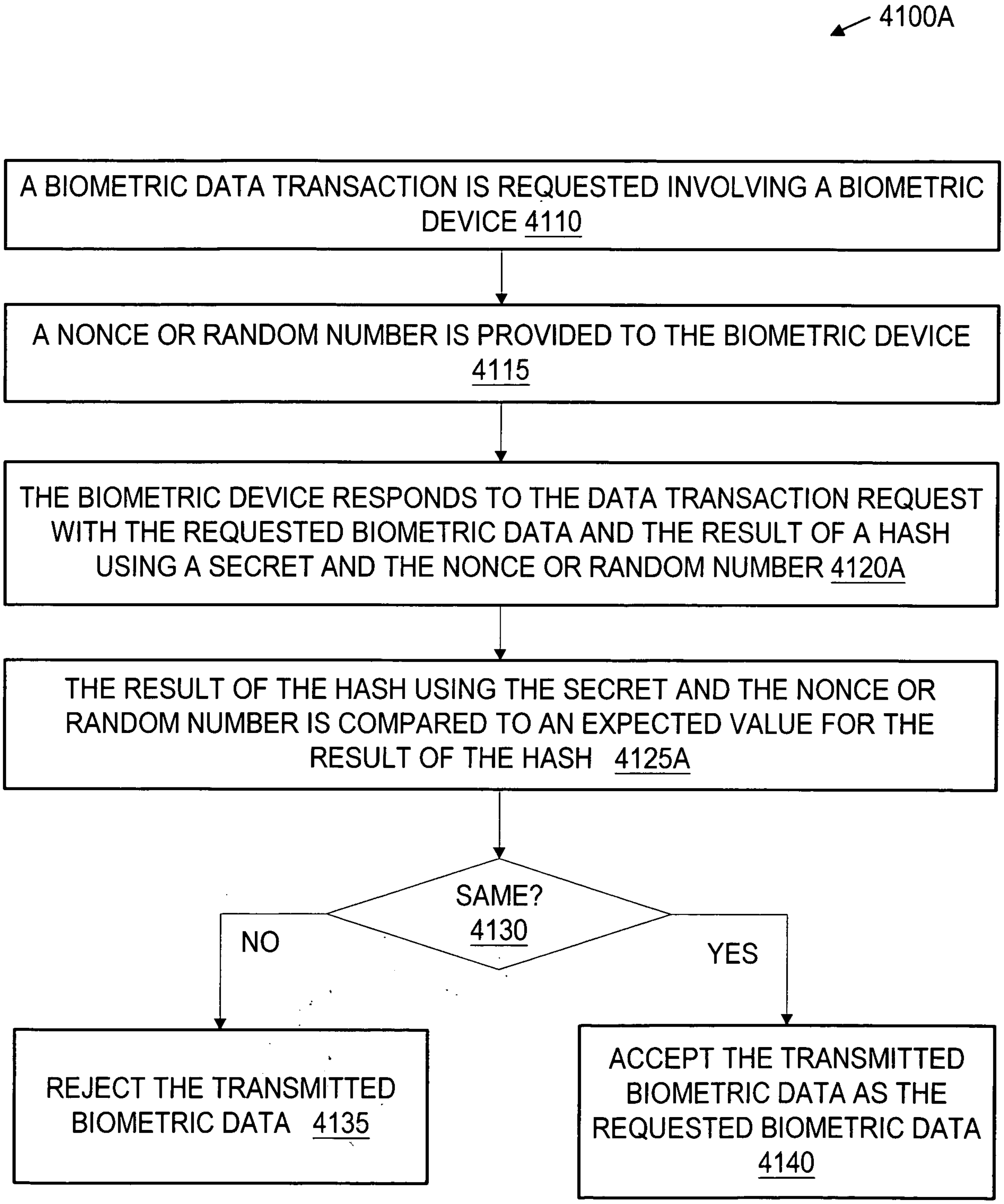

4100A
A BIOMETRIC DATA TRANSACTION IS REQUESTED INVOLVING A BIOMETRIC DEVICE 4110
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE BIOMETRIC DEVICE 4115
THE BIOMETRIC DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED BIOMETRIC DATA AND THE RESULT OF A HASH USING A SECRET AND THE NONCE OR RANDOM NUMBER 4120A
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4125A
SAME? 4130
NO
YES
REJECT THE TRANSMITTED BIOMETRIC DATA 4135
ACCEPT THE TRANSMITTED BIOMETRIC DATA AS THE REQUESTED BIOMETRIC DATA 4140

Fig. 30A

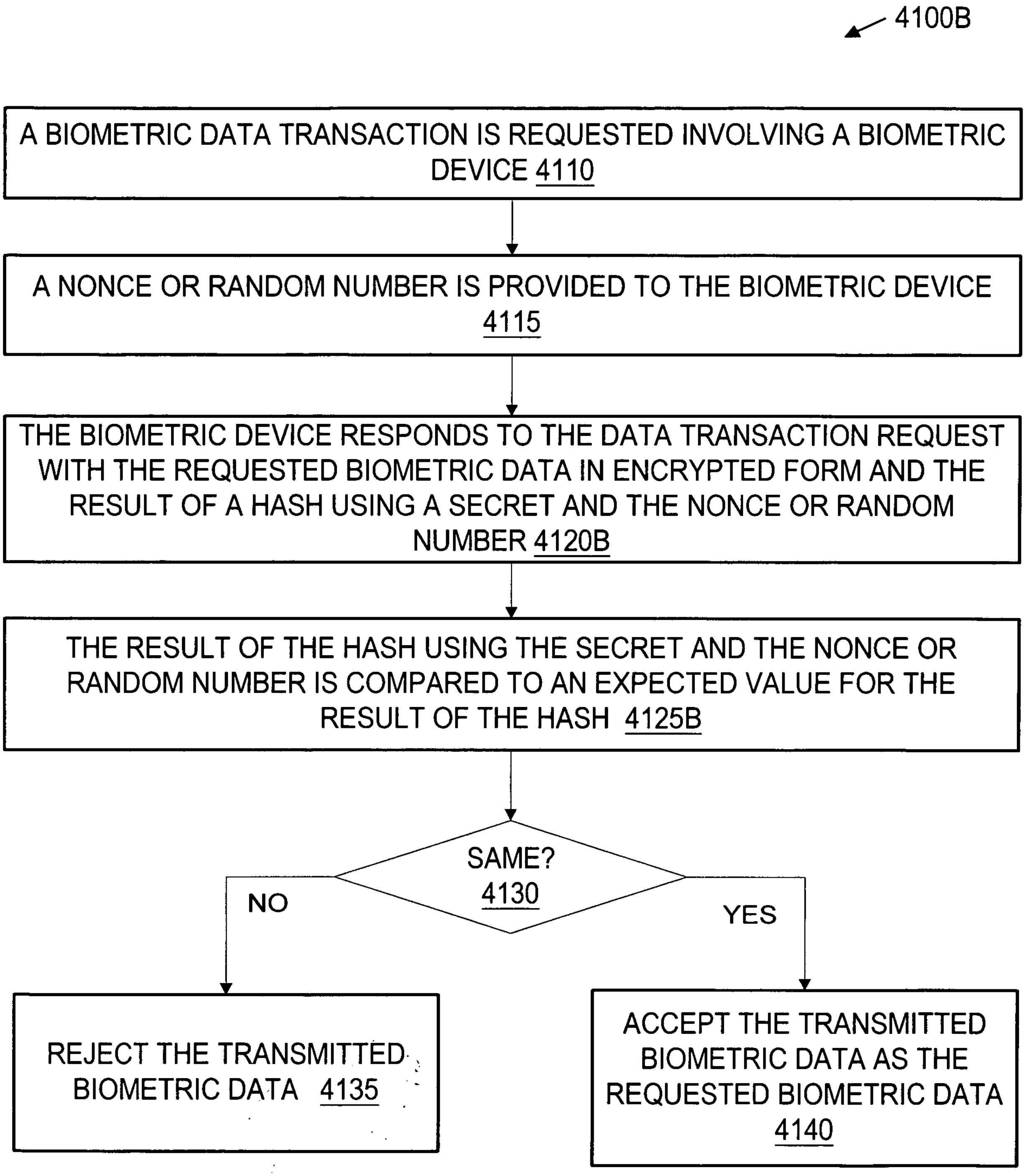

4100B
A BIOMETRIC DATA TRANSACTION IS REQUESTED INVOLVING A BIOMETRIC DEVICE 4110
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE BIOMETRIC DEVICE 4115
THE BIOMETRIC DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED BIOMETRIC DATA IN ENCRYPTED FORM AND THE RESULT OF A HASH USING A SECRET AND THE NONCE OR RANDOM NUMBER 4120B
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4125B
SAME? 4130
NO
YES
REJECT THE TRANSMITTED BIOMETRIC DATA 4135
ACCEPT THE TRANSMITTED BIOMETRIC DATA AS THE REQUESTED BIOMETRIC DATA 4140

Fig. 30B

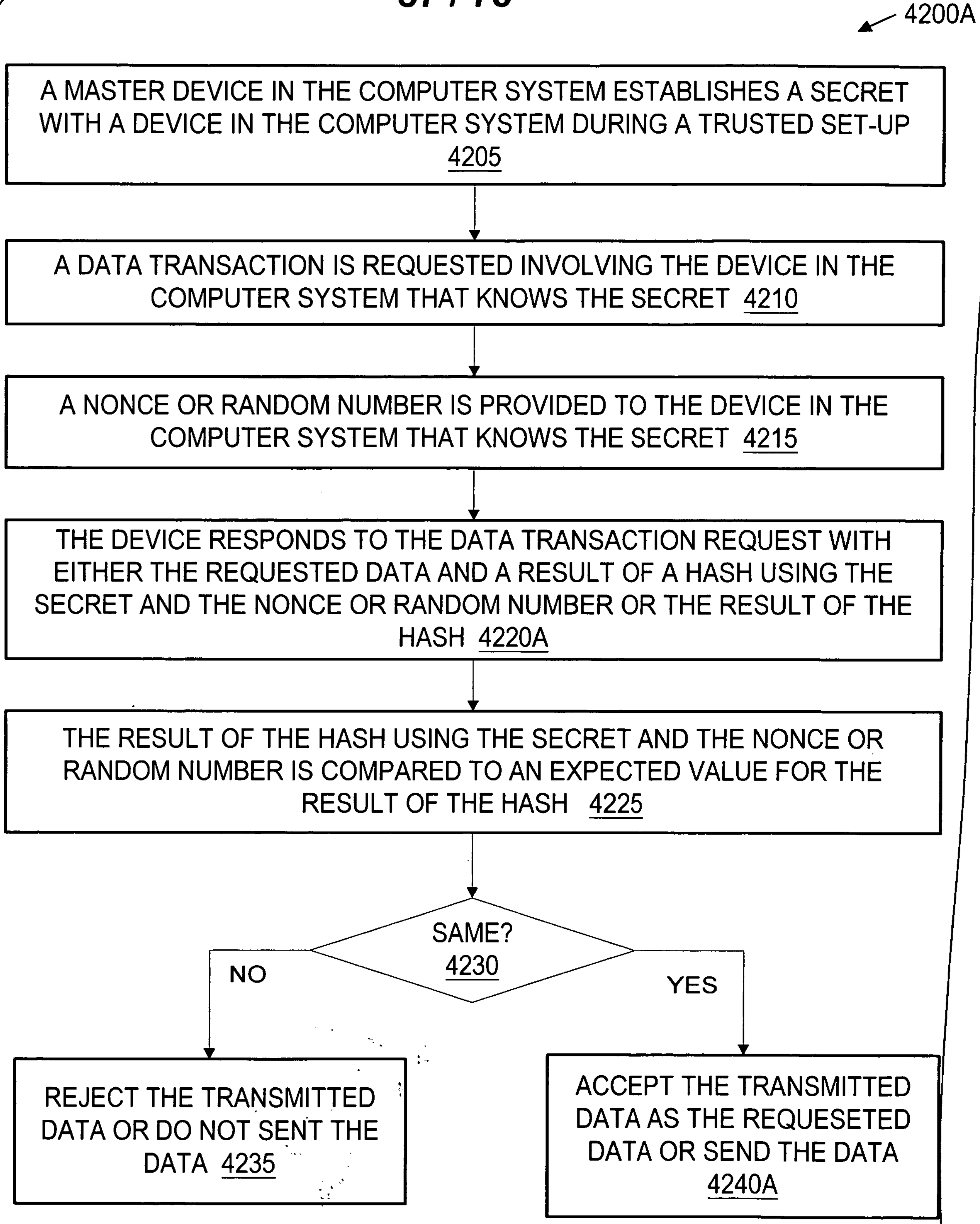

4200A
A MASTER DEVICE IN THE COMPUTER SYSTEM ESTABLISHES A SECRET WITH A DEVICE IN THE COMPUTER SYSTEM DURING A TRUSTED SET-UP 4205
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET 4210
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET 4215
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH EITHER THE REQUESTED DATA AND A RESULT OF A HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER OR THE RESULT OF THE HASH 4220A
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4225
SAME? 4230
NO
YES
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA 4235
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR SEND THE DATA 4240A

Fig. 31A

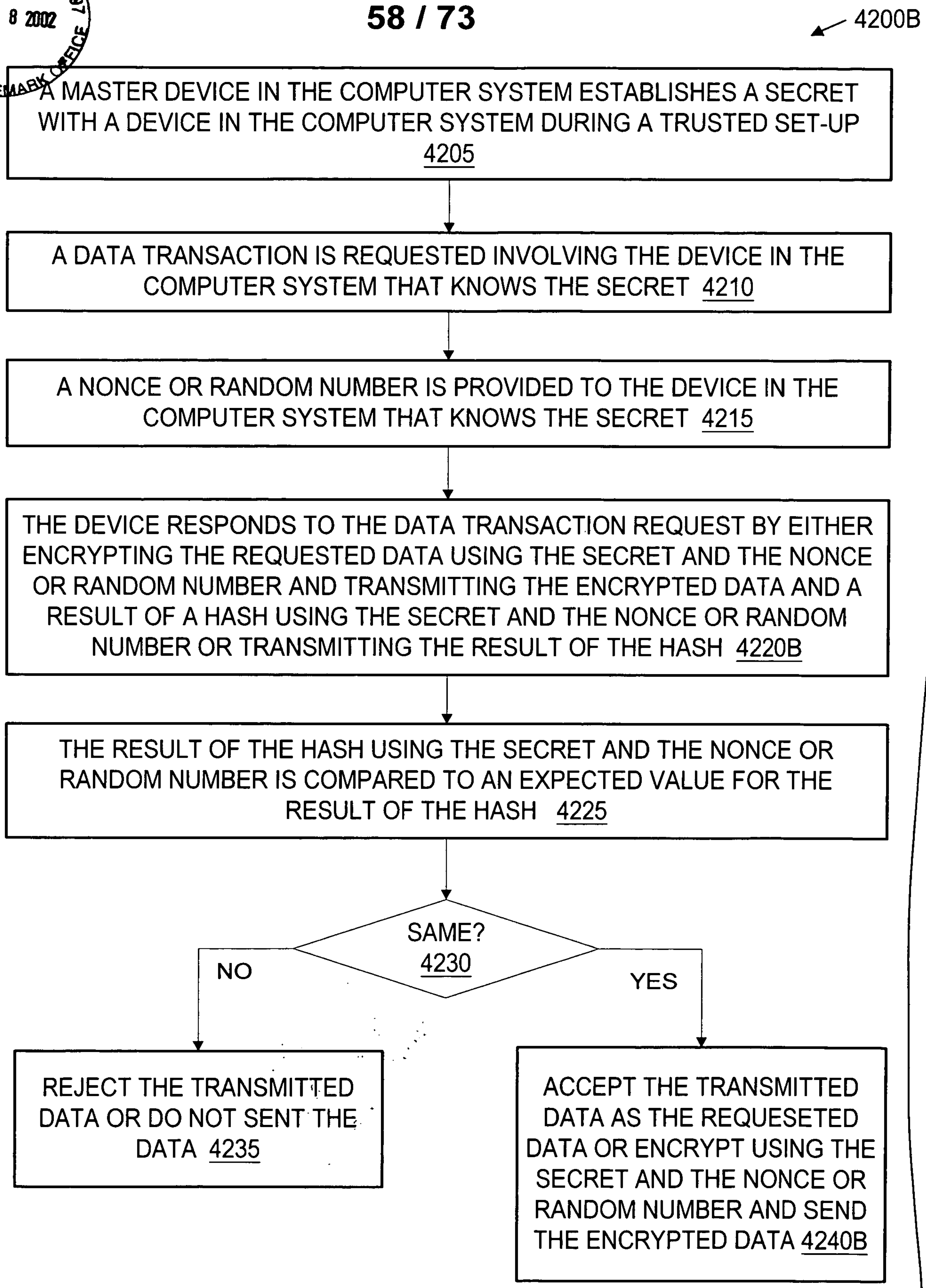

4200B
A MASTER DEVICE IN THE COMPUTER SYSTEM ESTABLISHES A SECRET WITH A DEVICE IN THE COMPUTER SYSTEM DURING A TRUSTED SET-UP 4205
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET 4210
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET 4215
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY EITHER ENCRYPTING THE REQUESTED DATA USING THE SECRET AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH 4220B
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4225
SAME? 4230
NO
YES
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA 4235
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR ENCRYPT USING THE SECRET AND THE NONCE OR RANDOM NUMBER AND SEND THE ENCRYPTED DATA 4240B

Fig. 31B

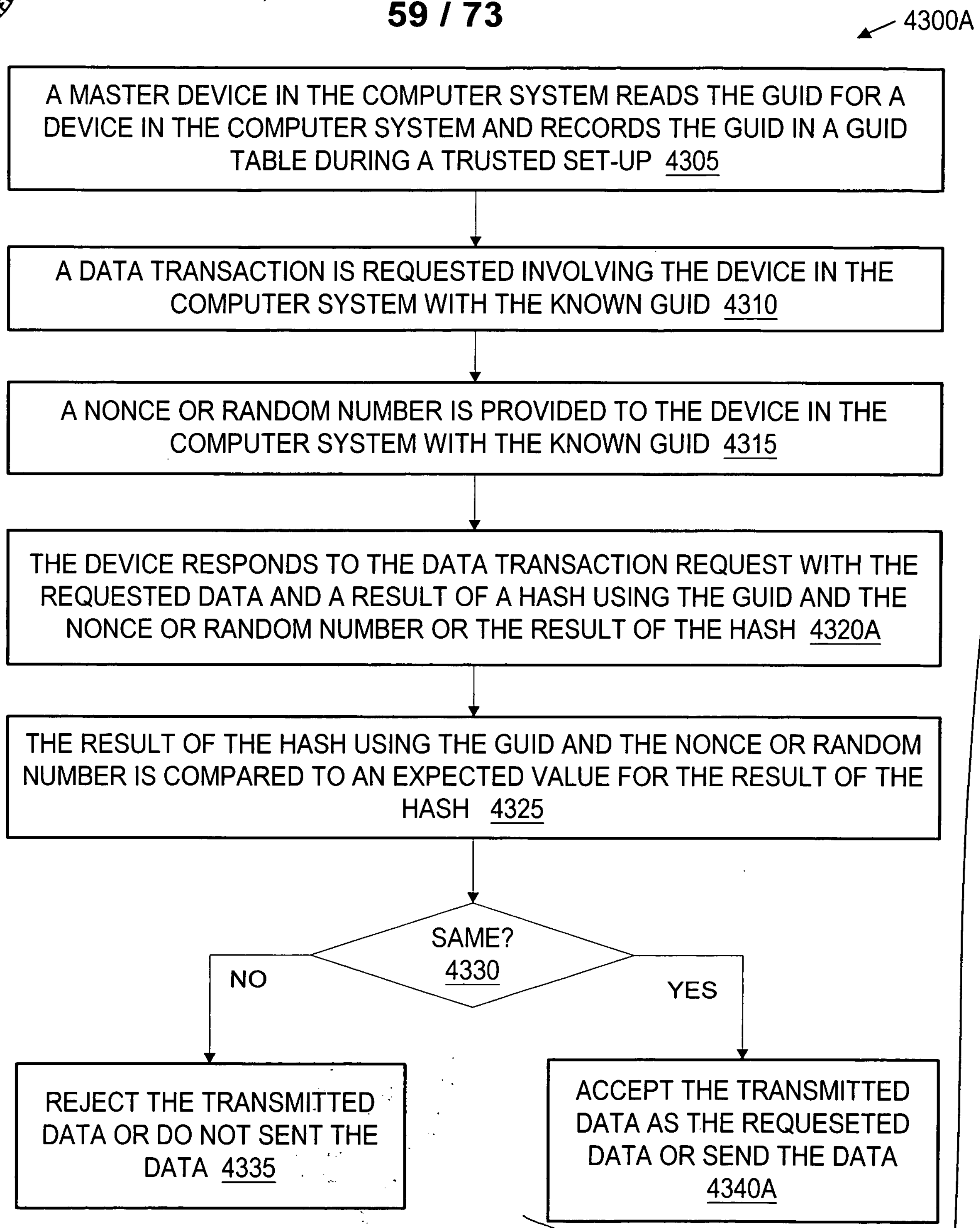

4300A
A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM AND RECORDS THE GUID IN A GUID TABLE DURING A TRUSTED SET-UP 4305
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4310
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4315
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED DATA AND A RESULT OF A HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER OR THE RESULT OF THE HASH 4320A
THE RESULT OF THE HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4325
SAME? 4330
NO
YES
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA 4335
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR SEND THE DATA 4340A

Fig. 32A

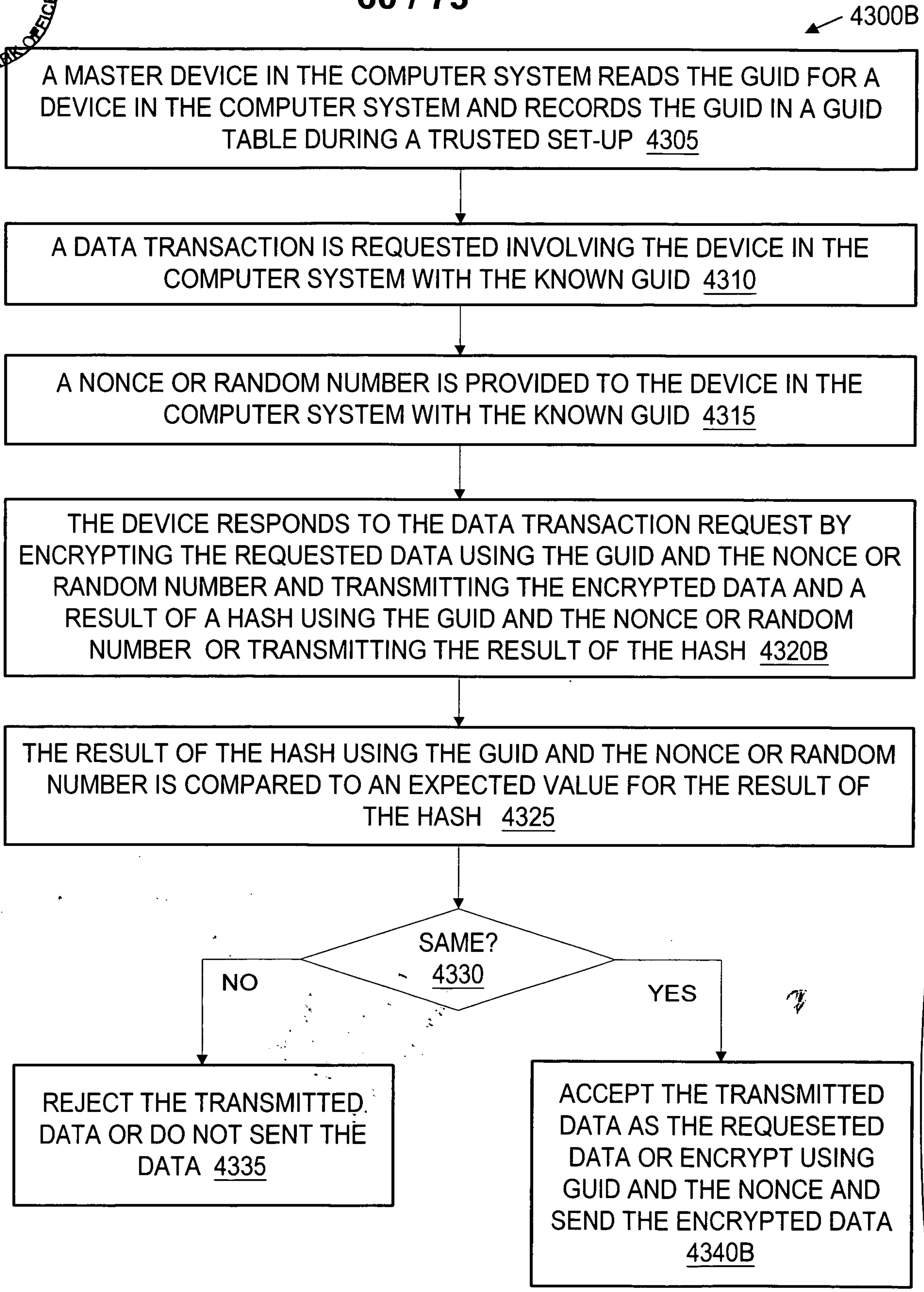

4300B
A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM AND RECORDS THE GUID IN A GUID TABLE DURING A TRUSTED SET-UP 4305
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4310
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4315
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY ENCRYPTING THE REQUESTED DATA USING THE GUID AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH 4320B
THE RESULT OF THE HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4325
SAME? 4330
NO
YES
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA 4335
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR ENCRYPT USING GUID AND THE NONCE AND SEND THE ENCRYPTED DATA 4340B

Fig. 32B

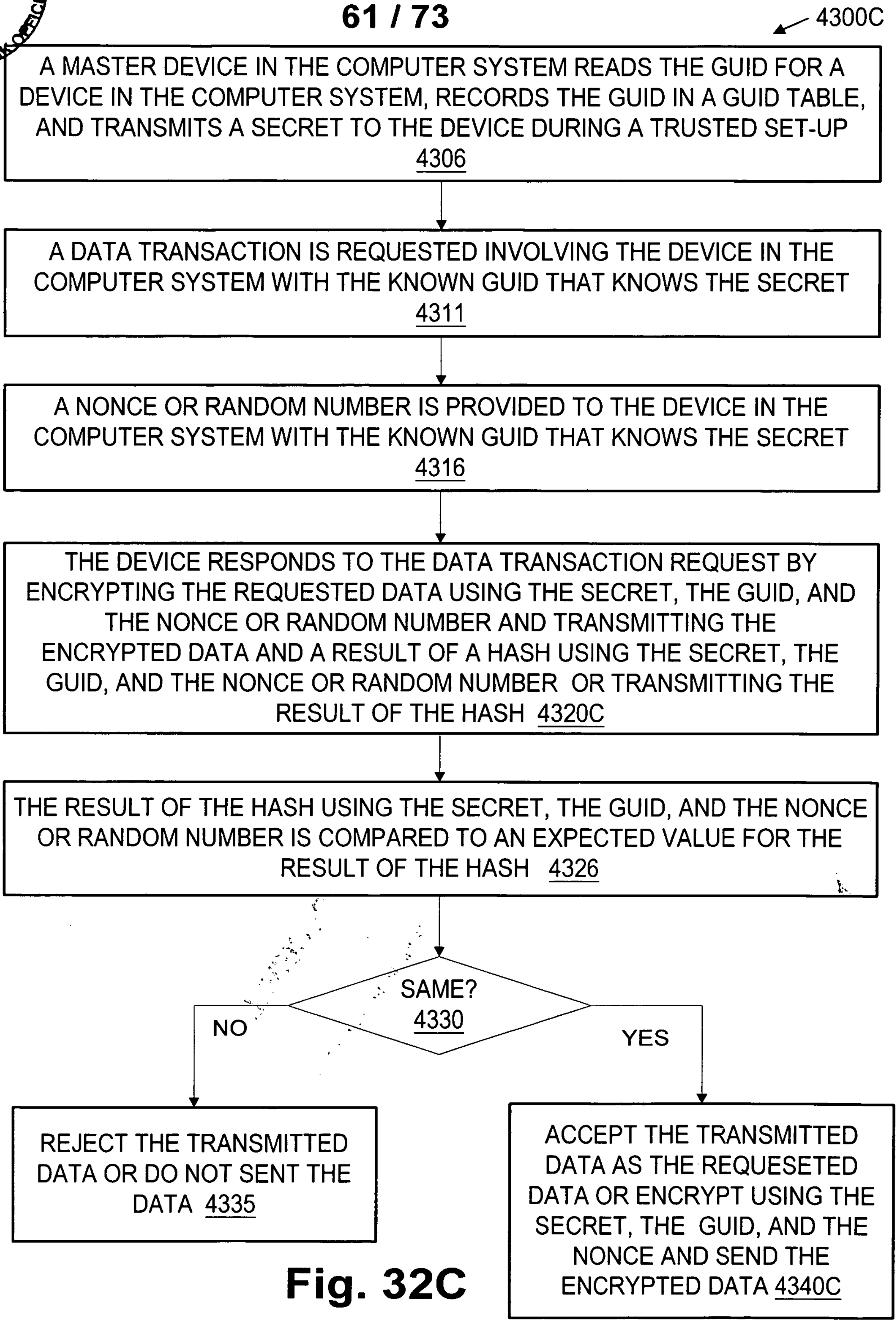

4300C
A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM, RECORDS THE GUID IN A GUID TABLE, AND TRANSMITS A SECRET TO THE DEVICE DURING A TRUSTED SET-UP 4306
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID THAT KNOWS THE SECRET 4311
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID THAT KNOWS THE SECRET 4316
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY ENCRYPTING THE REQUESTED DATA USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH 4320C
THE RESULT OF THE HASH USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4326
SAME? 4330
NO
YES
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA 4335
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR ENCRYPT USING THE SECRET, THE GUID, AND THE NONCE AND SEND THE ENCRYPTED DATA 4340C

Fig. 32C

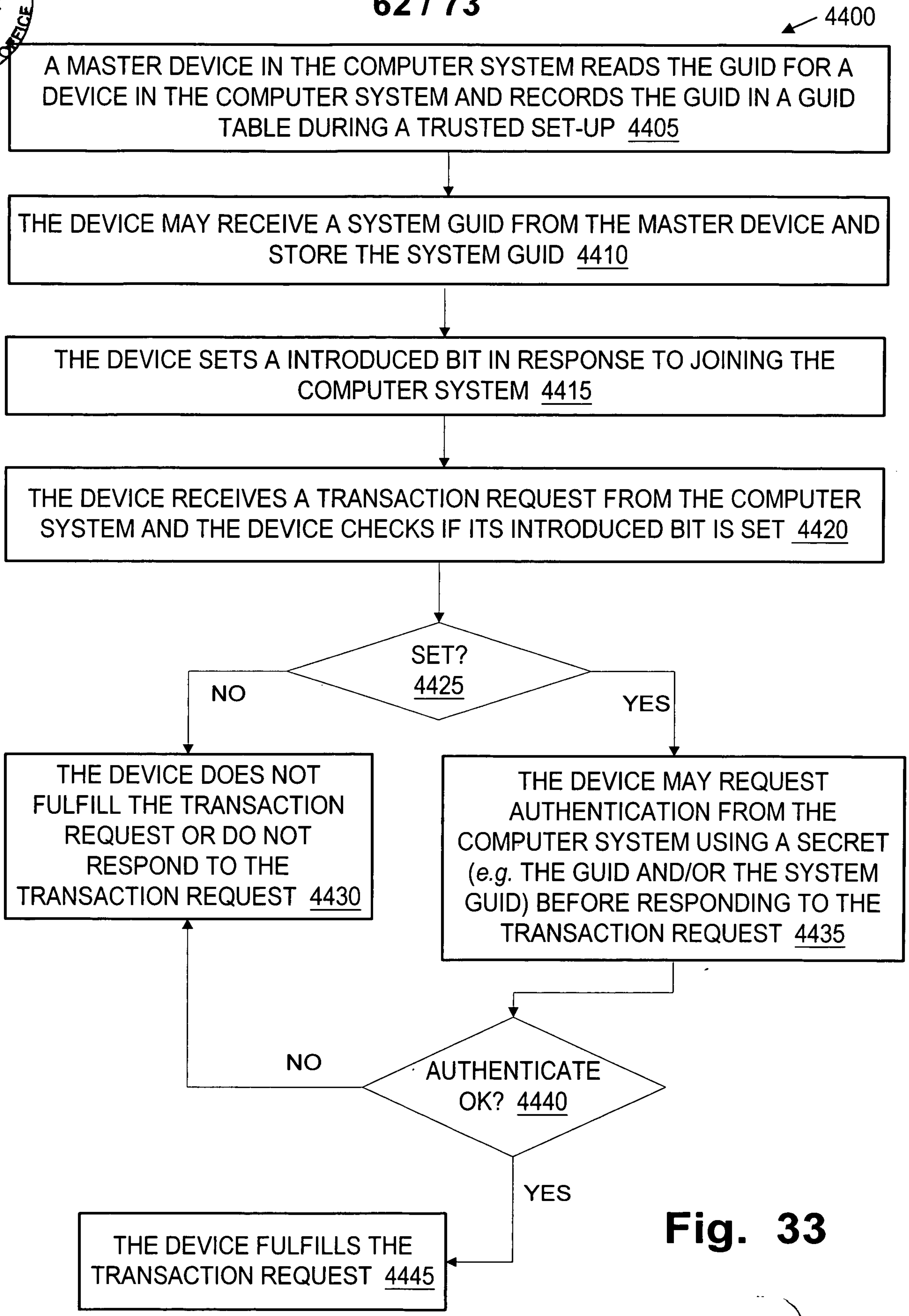
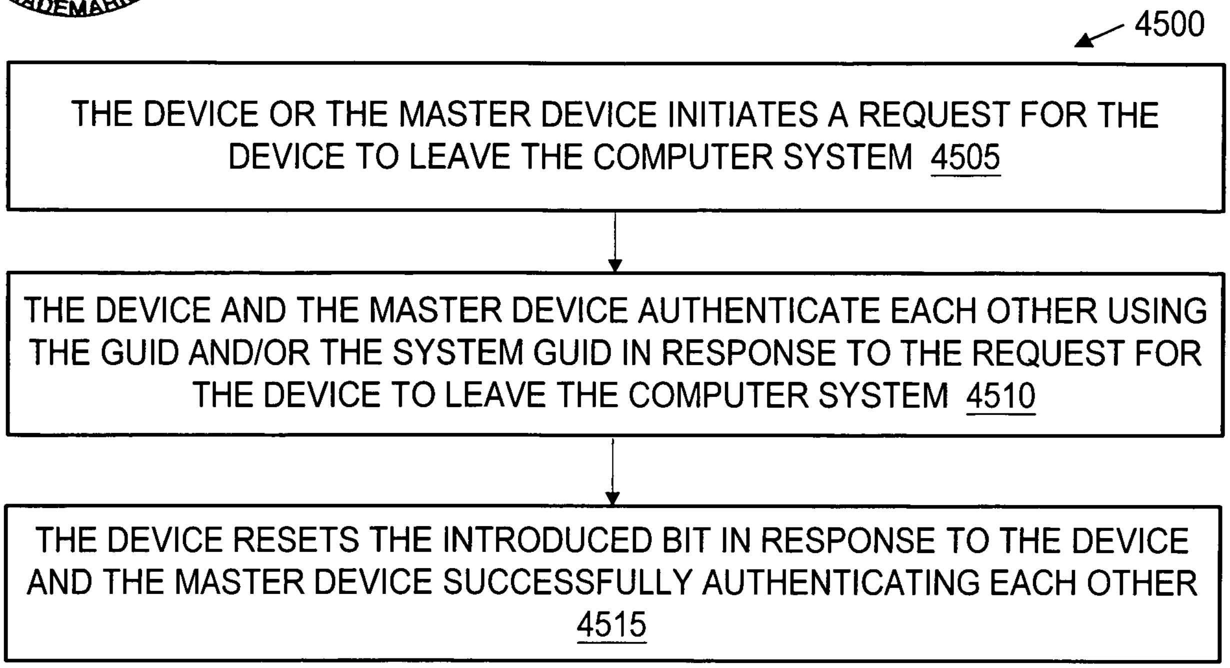

4400
A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM AND RECORDS THE GUID IN A GUID TABLE DURING A TRUSTED SET-UP 4405
THE DEVICE MAY RECEIVE A SYSTEM GUID FROM THE MASTER DEVICE AND STORE THE SYSTEM GUID 4410
THE DEVICE SETS A INTRODUCED BIT IN RESPONSE TO JOINING THE COMPUTER SYSTEM 4415
THE DEVICE RECEIVES A TRANSACTION REQUEST FROM THE COMPUTER SYSTEM AND THE DEVICE CHECKS IF ITS INTRODUCED BIT IS SET 4420
SET? 4425
NO
YES
THE DEVICE DOES NOT FULFILL THE TRANSACTION REQUEST OR DO NOT RESPOND TO THE TRANSACTION REQUEST 4430
THE DEVICE MAY REQUEST AUTHENTICATION FROM THE COMPUTER SYSTEM USING A SECRET (*e.g.* THE GUID AND/OR THE SYSTEM GUID) BEFORE RESPONDING TO THE TRANSACTION REQUEST 4435
NO
AUTHENTICATE OK? 4440
YES
THE DEVICE FULFILLS THE TRANSACTION REQUEST 4445

Fig. 33

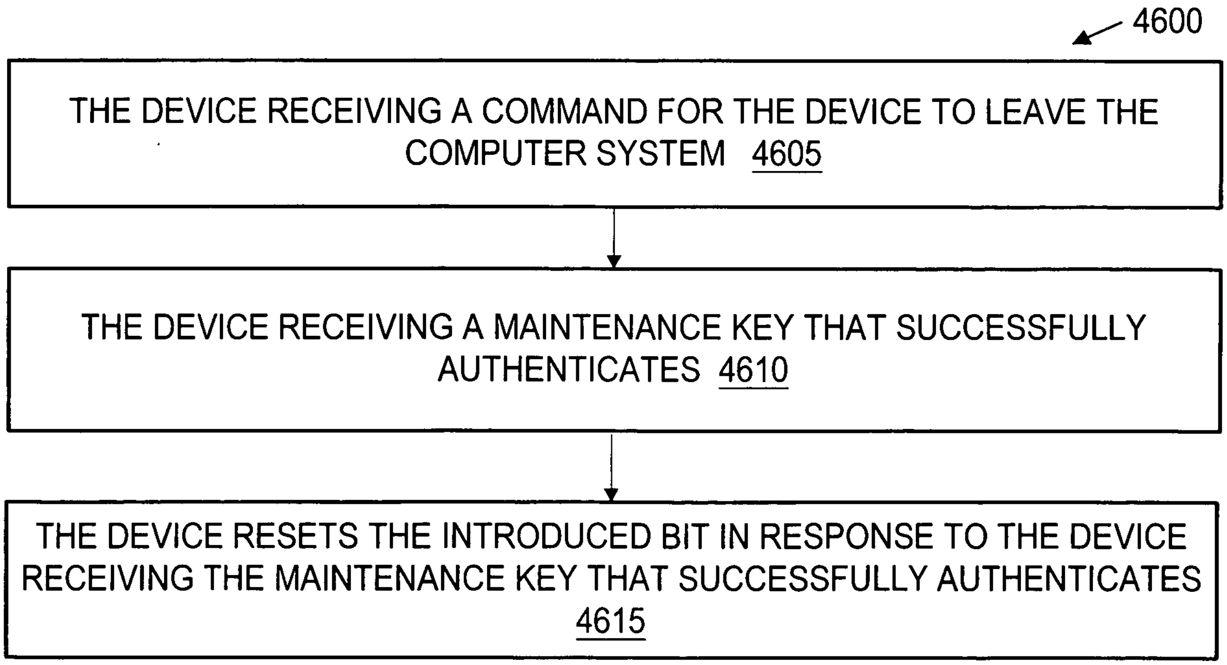


THE DEVICE OR THE MASTER DEVICE INITIATES A REQUEST FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM 4505

THE DEVICE AND THE MASTER DEVICE AUTHENTICATE EACH OTHER USING THE GUID AND/OR THE SYSTEM GUID IN RESPONSE TO THE REQUEST FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM 4510

THE DEVICE RESETS THE INTRODUCED BIT IN RESPONSE TO THE DEVICE AND THE MASTER DEVICE SUCCESSFULLY AUTHENTICATING EACH OTHER 4515

Fig. 34



THE DEVICE RECEIVING A COMMAND FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM 4605

THE DEVICE RECEIVING A MAINTENANCE KEY THAT SUCCESSFULLY AUTHENTICATES 4610

THE DEVICE RESETS THE INTRODUCED BIT IN RESPONSE TO THE DEVICE RECEIVING THE MAINTENANCE KEY THAT SUCCESSFULLY AUTHENTICATES 4615

Fig. 35

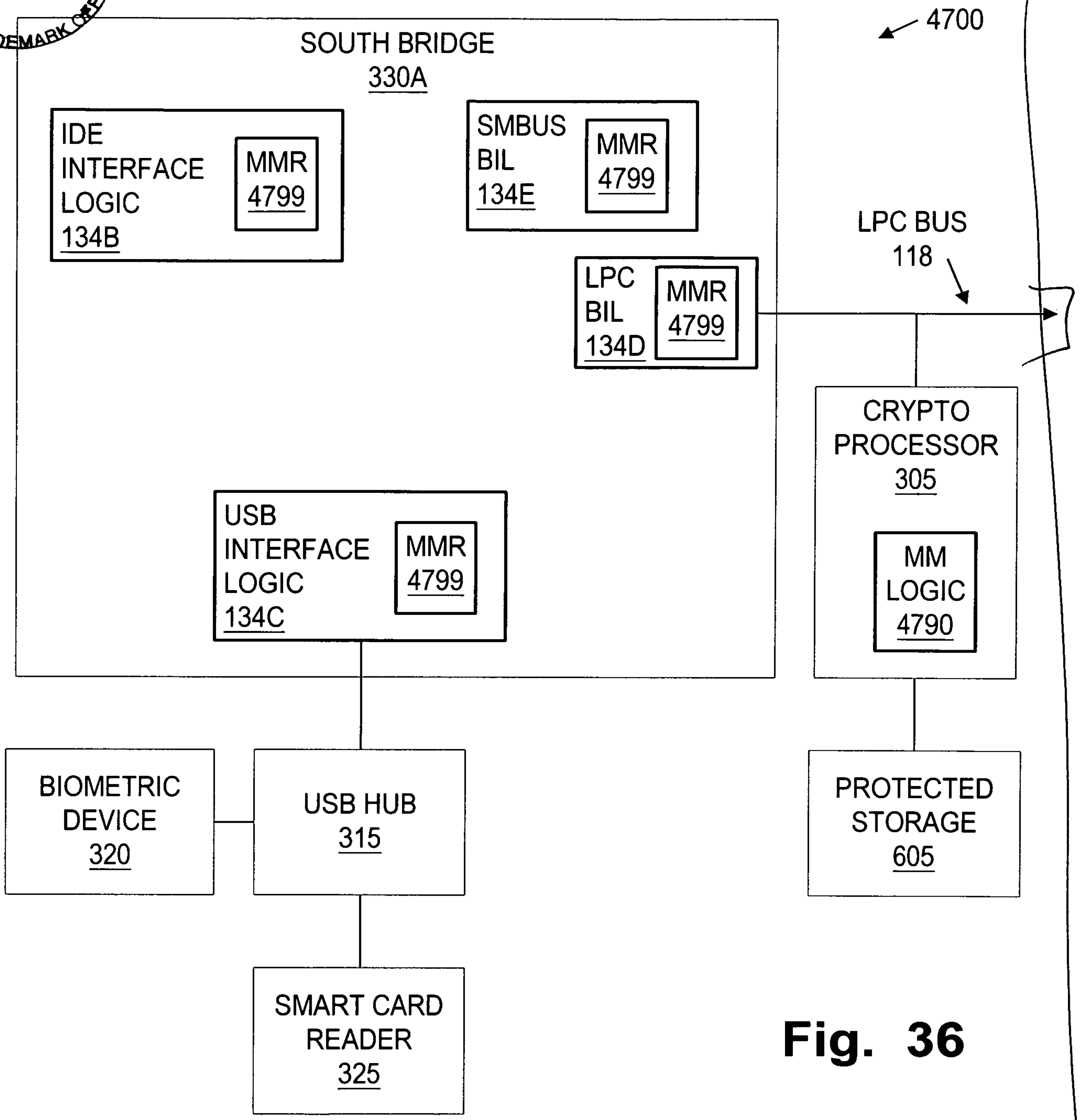

4700
SOUTH BRIDGE
330A
IDE
INTERFACE
LOGIC
134B
MMR
4799
SMBUS
BIL
134E
MMR
4799
LPC
BIL
134D
MMR
4799
LPC BUS
118
USB
INTERFACE
LOGIC
134C
MMR
4799
CRYPTO
PROCESSOR
305
MM
LOGIC
4790
BIOMETRIC
DEVICE
320
USB HUB
315
PROTECTED
STORAGE
605
SMART CARD
READER
325

Fig. 36

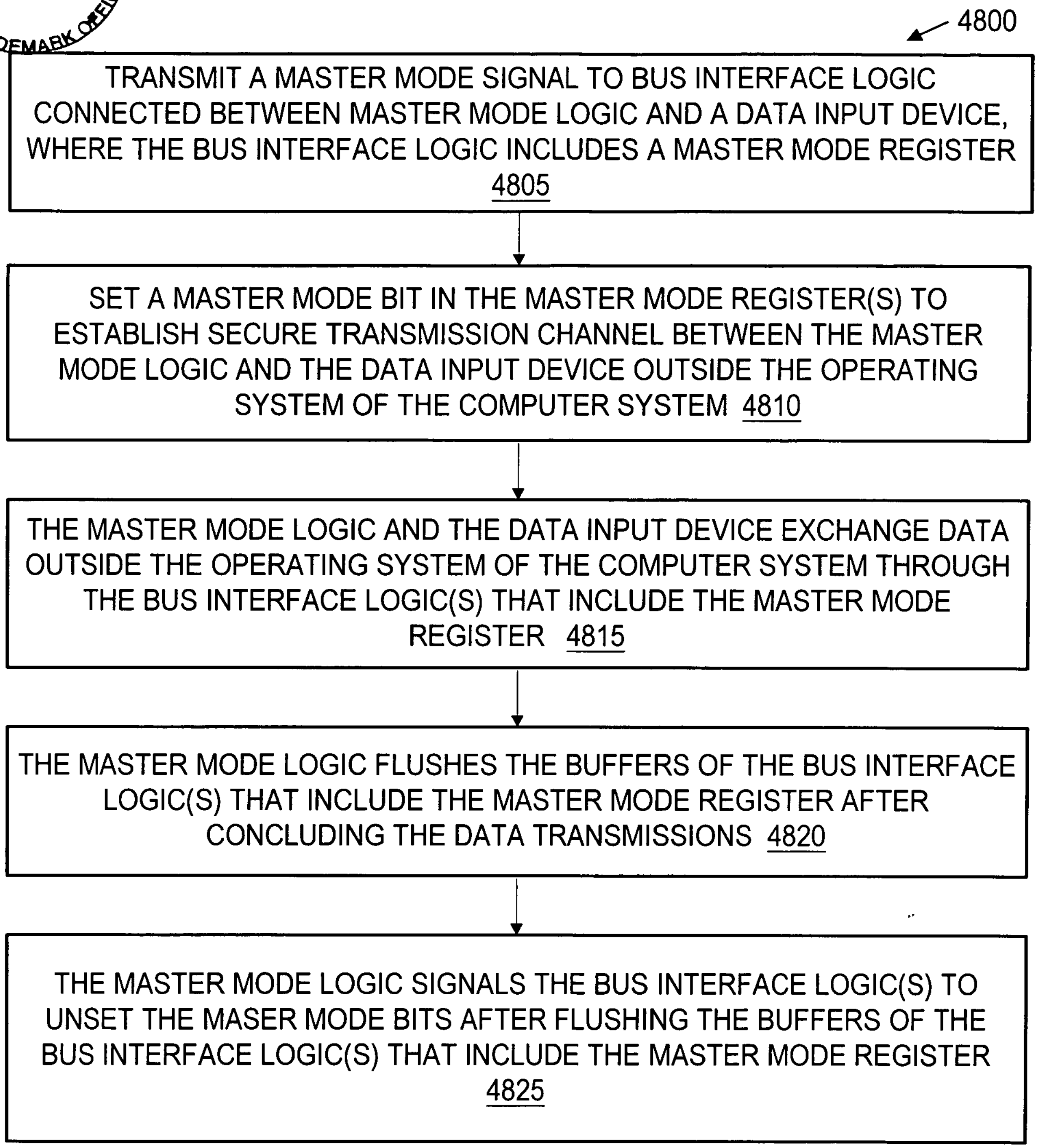

4800
TRANSMIT A MASTER MODE SIGNAL TO BUS INTERFACE LOGIC CONNECTED BETWEEN MASTER MODE LOGIC AND A DATA INPUT DEVICE, WHERE THE BUS INTERFACE LOGIC INCLUDES A MASTER MODE REGISTER 4805
SET A MASTER MODE BIT IN THE MASTER MODE REGISTER(S) TO ESTABLISH SECURE TRANSMISSION CHANNEL BETWEEN THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM 4810
THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE EXCHANGE DATA OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM THROUGH THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER 4815
THE MASTER MODE LOGIC FLUSHES THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER AFTER CONCLUDING THE DATA TRANSMISSIONS 4820
THE MASTER MODE LOGIC SIGNALS THE BUS INTERFACE LOGIC(S) TO UNSET THE MASER MODE BITS AFTER FLUSHING THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER 4825

Fig. 37

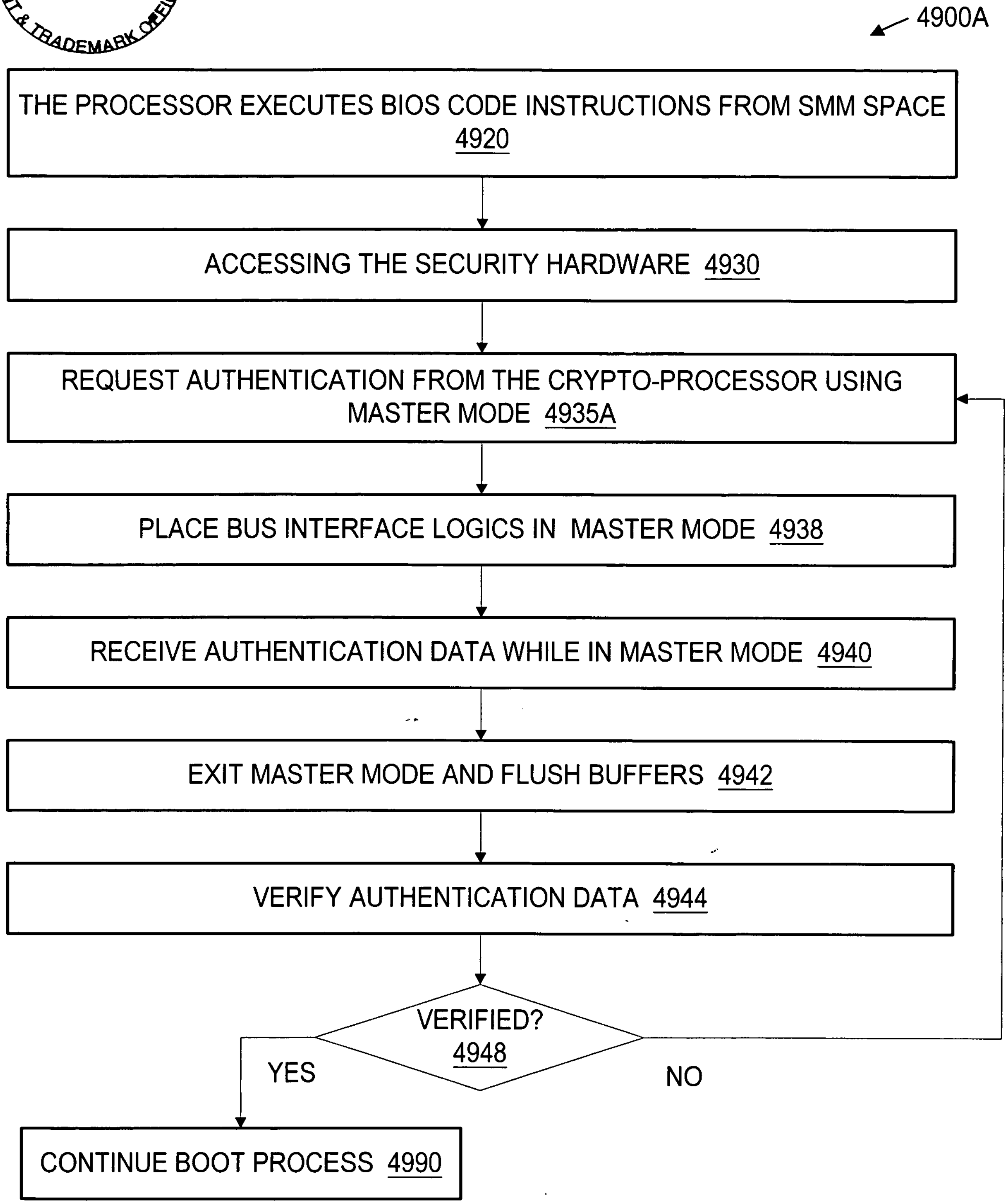

4900A
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE 4920
ACCESSING THE SECURITY HARDWARE 4930
REQUEST AUTHENTICATION FROM THE CRYPTO-PROCESSOR USING MASTER MODE 4935A
PLACE BUS INTERFACE LOGICS IN MASTER MODE 4938
RECEIVE AUTHENTICATION DATA WHILE IN MASTER MODE 4940
EXIT MASTER MODE AND FLUSH BUFFERS 4942
VERIFY AUTHENTICATION DATA 4944
VERIFIED? 4948
YES
NO
CONTINUE BOOT PROCESS 4990

Fig. 38A

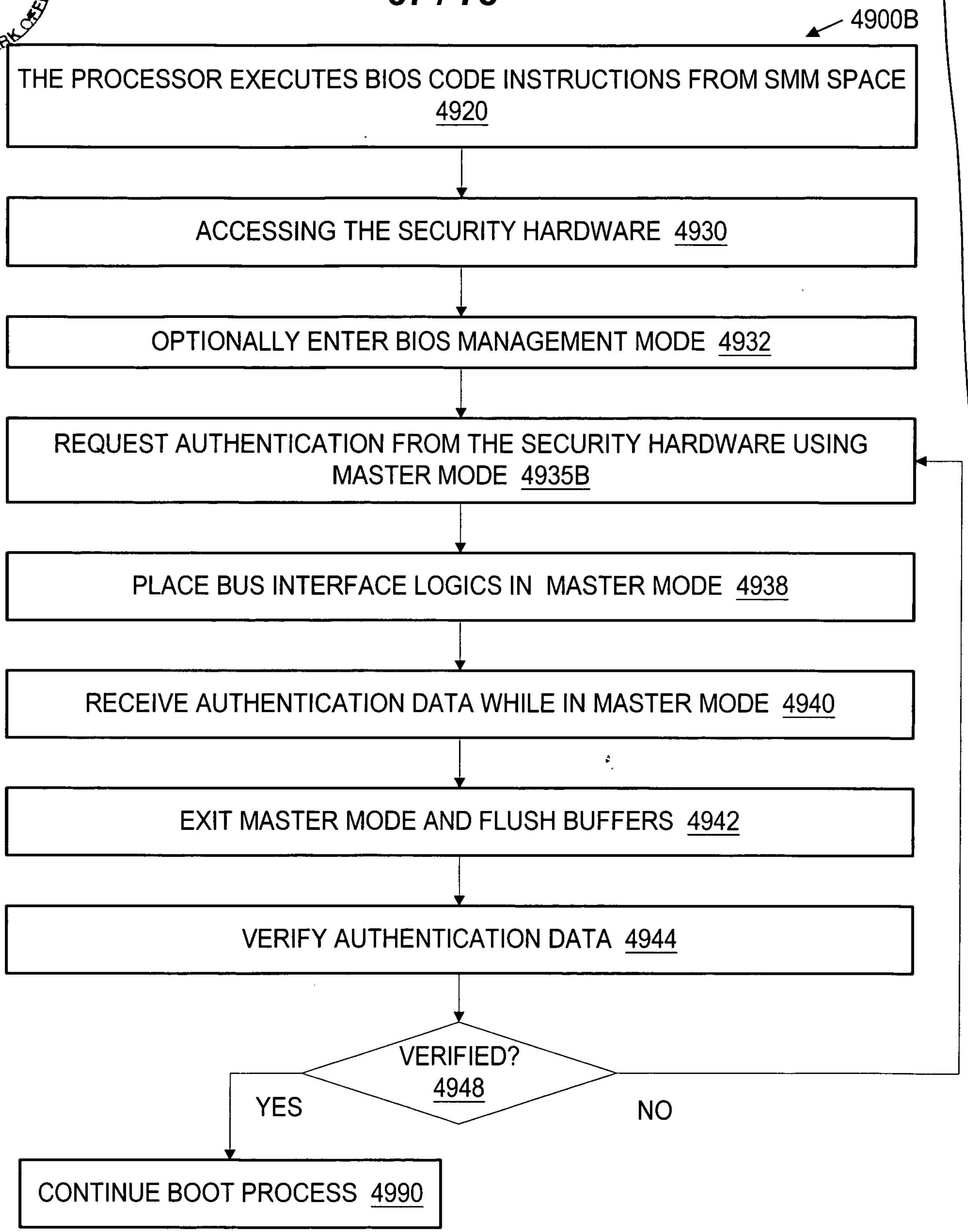

4900B
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE 4920
ACCESSING THE SECURITY HARDWARE 4930
OPTIONALLY ENTER BIOS MANAGEMENT MODE 4932
REQUEST AUTHENTICATION FROM THE SECURITY HARDWARE USING MASTER MODE 4935B
PLACE BUS INTERFACE LOGICS IN MASTER MODE 4938
RECEIVE AUTHENTICATION DATA WHILE IN MASTER MODE 4940
EXIT MASTER MODE AND FLUSH BUFFERS 4942
VERIFY AUTHENTICATION DATA 4944
VERIFIED? 4948
YES
NO
CONTINUE BOOT PROCESS 4990

Fig. 38B

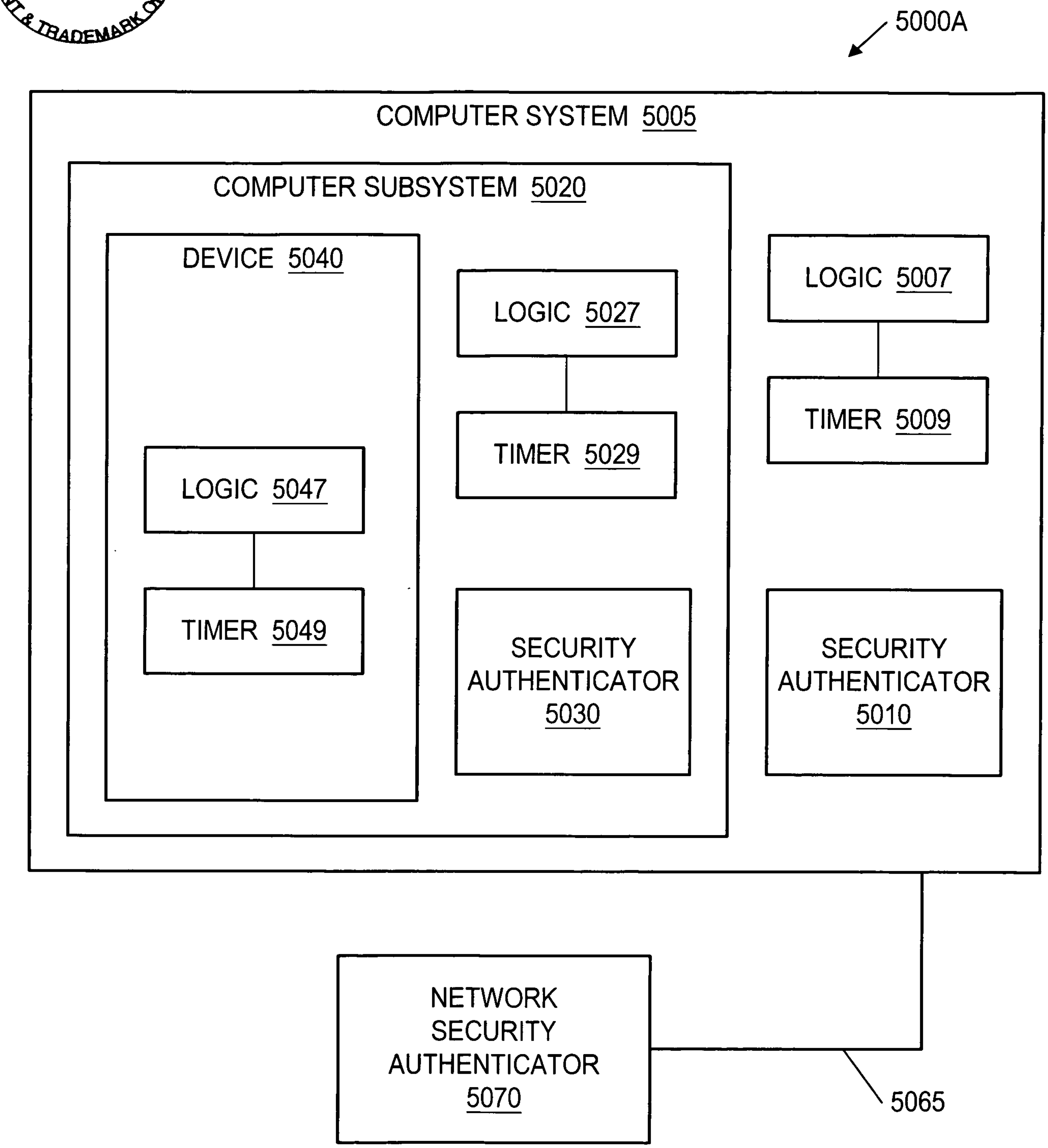

5000A
COMPUTER SYSTEM 5005
COMPUTER SUBSYSTEM 5020
DEVICE 5040
LOGIC 5047
TIMER 5049
LOGIC 5027
TIMER 5029
SECURITY AUTHENTICATOR 5030
LOGIC 5007
TIMER 5009
SECURITY AUTHENTICATOR 5010
NETWORK SECURITY AUTHENTICATOR 5070
5065

Fig. 39A

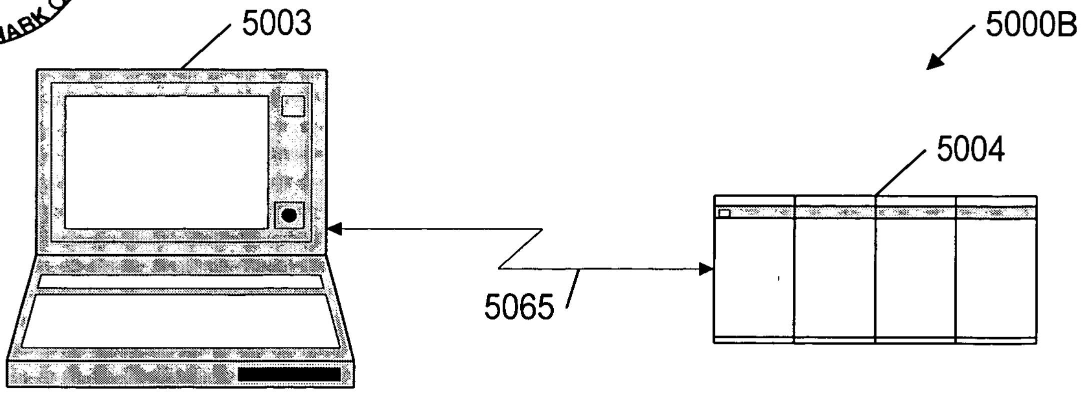


Fig. 39B

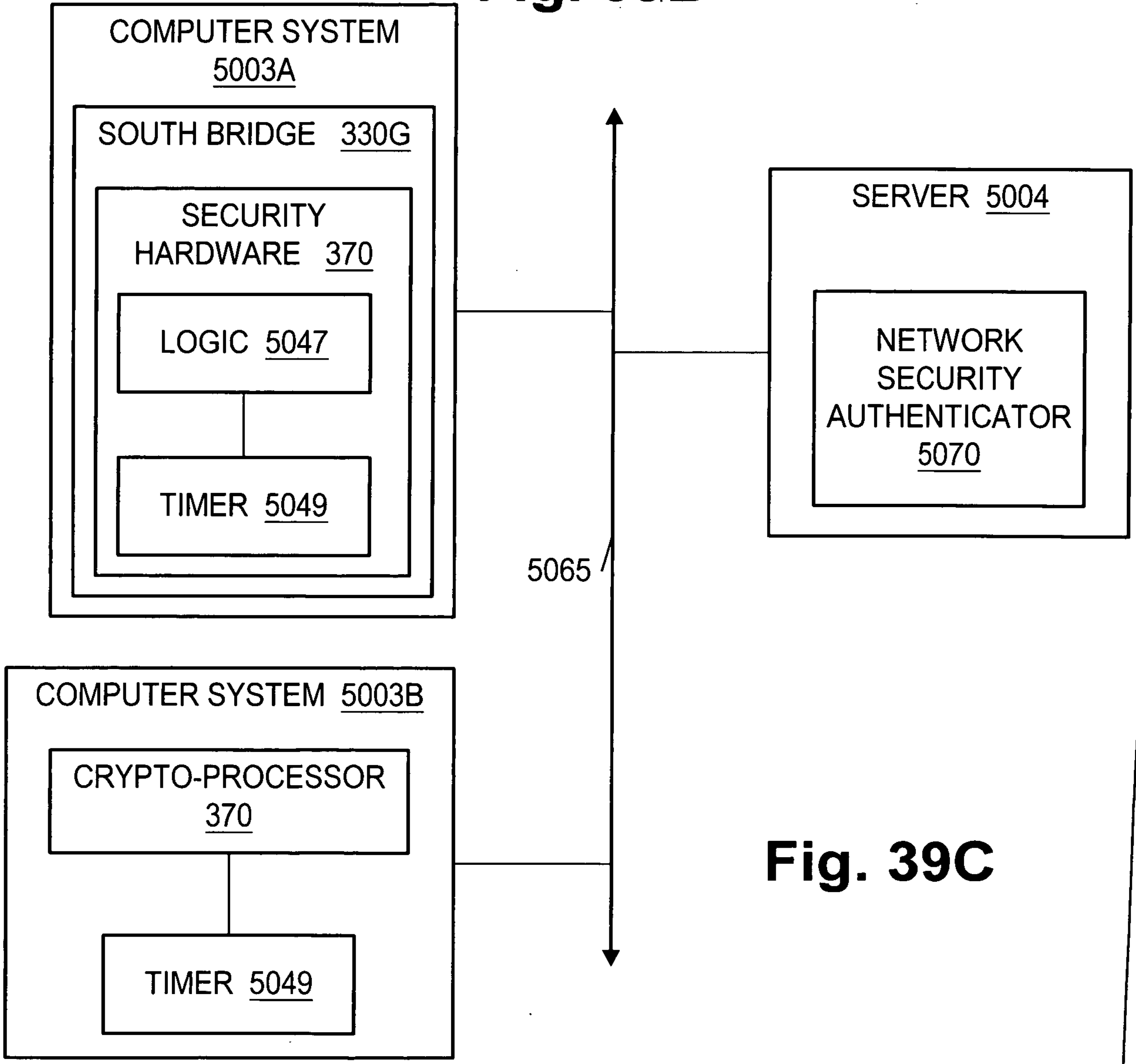


Fig. 39C

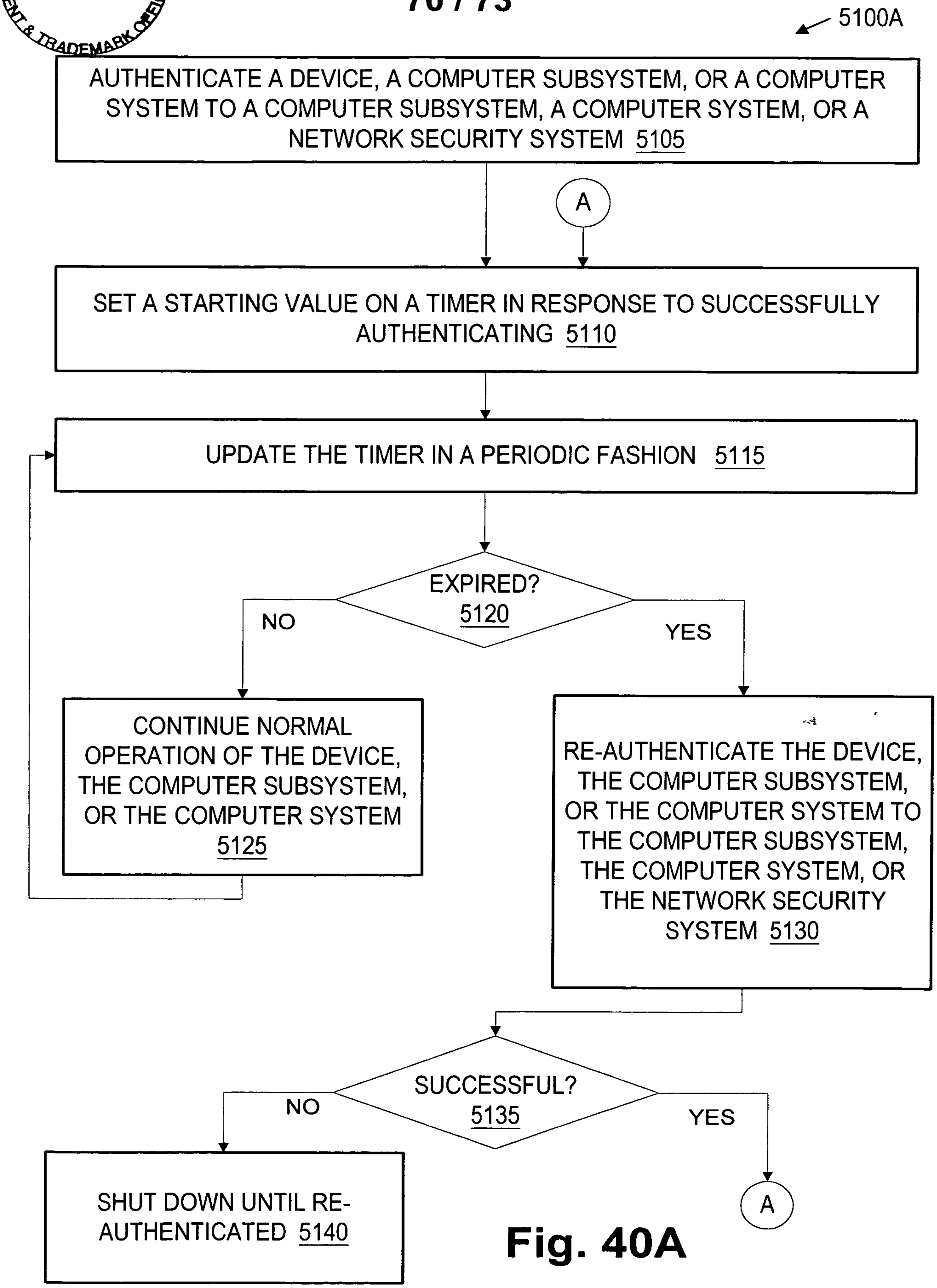

5100A
AUTHENTICATE A DEVICE, A COMPUTER SUBSYSTEM, OR A COMPUTER SYSTEM TO A COMPUTER SUBSYSTEM, A COMPUTER SYSTEM, OR A NETWORK SECURITY SYSTEM 5105
A
SET A STARTING VALUE ON A TIMER IN RESPONSE TO SUCCESSFULLY AUTHENTICATING 5110
UPDATE THE TIMER IN A PERIODIC FASHION 5115
EXPIRED? 5120
NO
YES
CONTINUE NORMAL OPERATION OF THE DEVICE, THE COMPUTER SUBSYSTEM, OR THE COMPUTER SYSTEM 5125
RE-AUTHENTICATE THE DEVICE, THE COMPUTER SUBSYSTEM, OR THE COMPUTER SYSTEM TO THE COMPUTER SUBSYSTEM, THE COMPUTER SYSTEM, OR THE NETWORK SECURITY SYSTEM 5130
SUCCESSFUL? 5135
NO
YES
SHUT DOWN UNTIL RE-AUTHENTICATED 5140
A

Fig. 40A

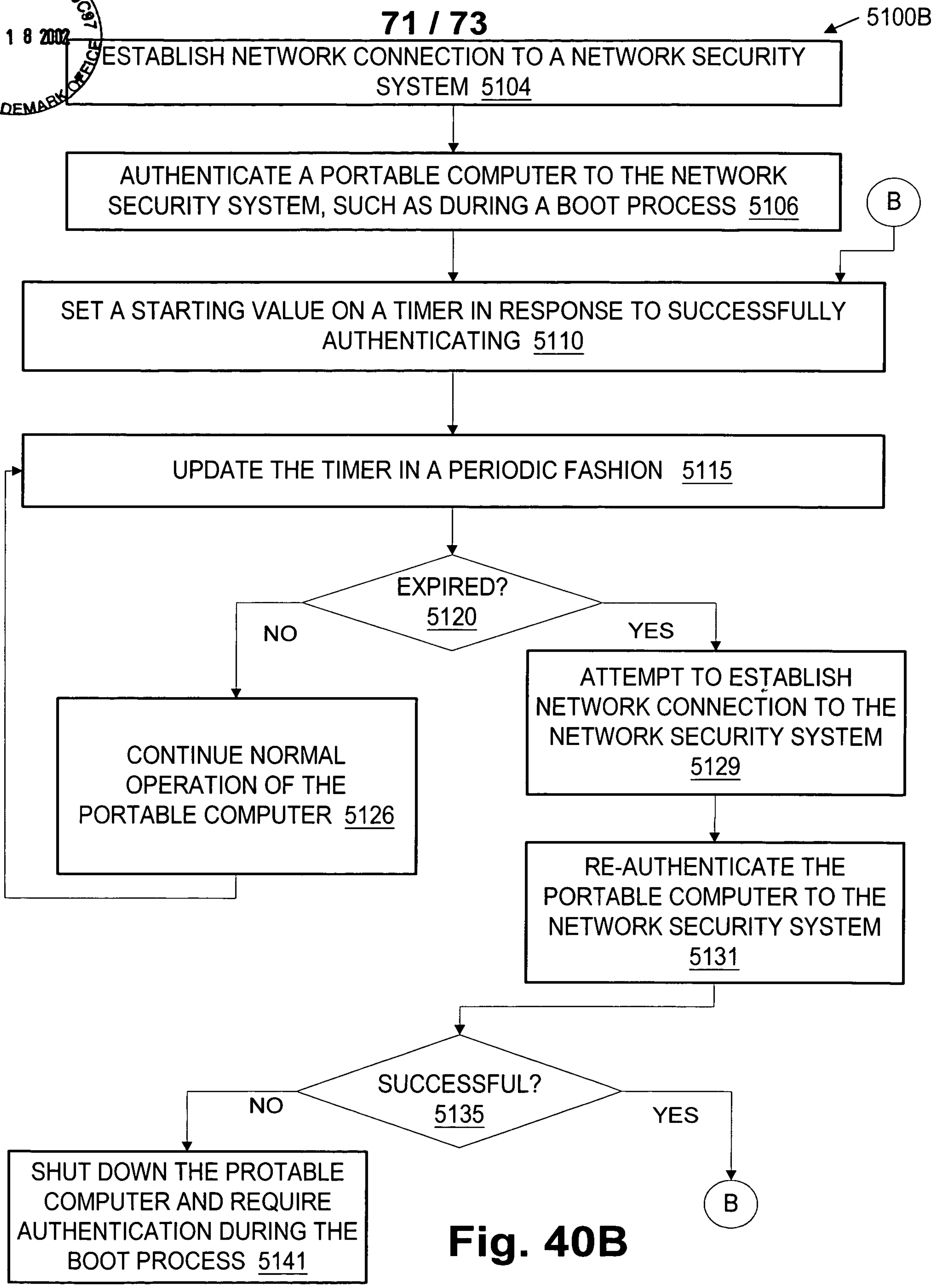

5100B
ESTABLISH NETWORK CONNECTION TO A NETWORK SECURITY SYSTEM 5104
AUTHENTICATE A PORTABLE COMPUTER TO THE NETWORK SECURITY SYSTEM, SUCH AS DURING A BOOT PROCESS 5106
B
SET A STARTING VALUE ON A TIMER IN RESPONSE TO SUCCESSFULLY AUTHENTICATING 5110
UPDATE THE TIMER IN A PERIODIC FASHION 5115
EXPIRED? 5120
NO
YES
CONTINUE NORMAL OPERATION OF THE PORTABLE COMPUTER 5126
ATTEMPT TO ESTABLISH NETWORK CONNECTION TO THE NETWORK SECURITY SYSTEM 5129
RE-AUTHENTICATE THE PORTABLE COMPUTER TO THE NETWORK SECURITY SYSTEM 5131
SUCCESSFUL? 5135
NO
YES
SHUT DOWN THE PROTABLE COMPUTER AND REQUIRE AUTHENTICATION DURING THE BOOT PROCESS 5141
B

Fig. 40B

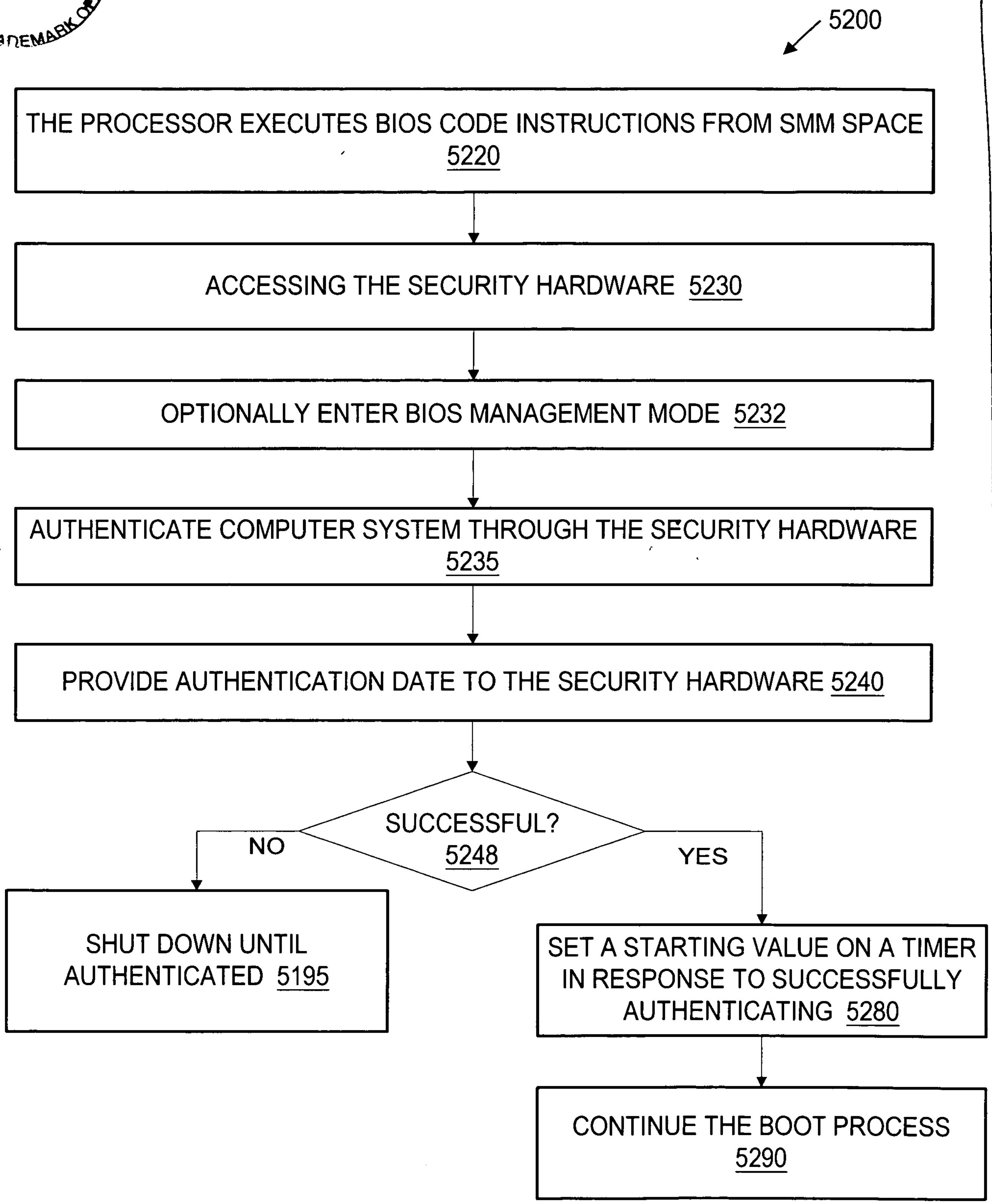

5200
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE 5220
ACCESSING THE SECURITY HARDWARE 5230
OPTIONALLY ENTER BIOS MANAGEMENT MODE 5232
AUTHENTICATE COMPUTER SYSTEM THROUGH THE SECURITY HARDWARE 5235
PROVIDE AUTHENTICATION DATE TO THE SECURITY HARDWARE 5240
SUCCESSFUL? 5248
NO
YES
SHUT DOWN UNTIL AUTHENTICATED 5195
SET A STARTING VALUE ON A TIMER IN RESPONSE TO SUCCESSFULLY AUTHENTICATING 5280
CONTINUE THE BOOT PROCESS 5290

Fig. 41

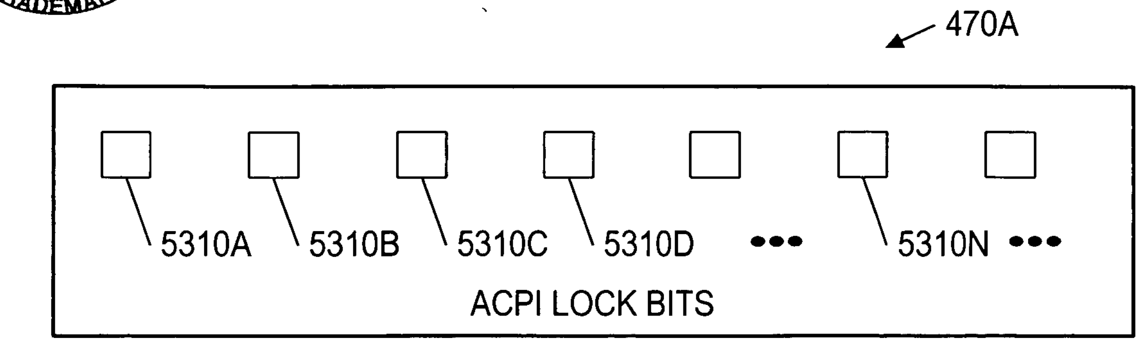


Fig. 42A

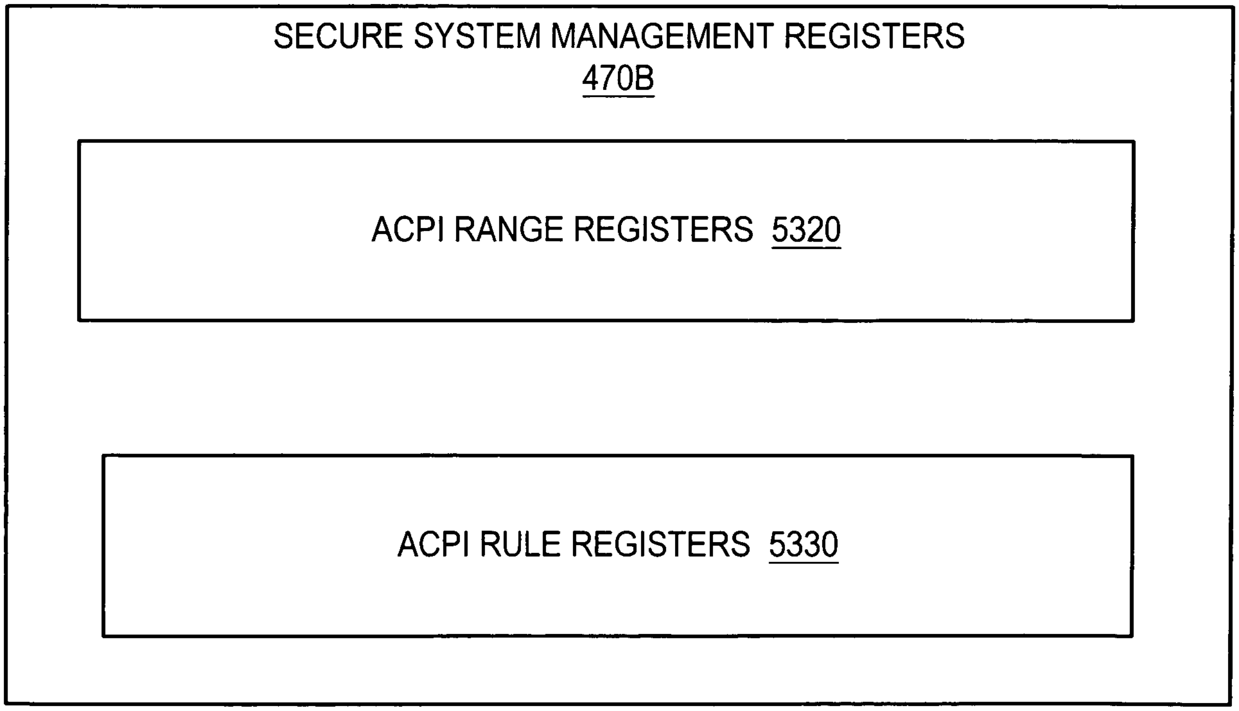


Fig. 42B